

Studies in Computational Intelligence, Volume 334

Editor-in-Chief

Prof. Janusz Kacprzyk
Systems Research Institute
Polish Academy of Sciences
ul. Newelska 6
01-447 Warsaw
Poland
E-mail: kacprzyk@ibspan.waw.pl

Further volumes of this series can be found on our homepage: springer.com

Vol. 312. Patricia Melin, Janusz Kacprzyk, and Witold Pedrycz (Eds.)
Soft Computing for Recognition based on Biometrics, 2010
ISBN 978-3-642-15110-1

Vol. 313. Imre J. Rudas, János Fodor, and Janusz Kacprzyk (Eds.)
Computational Intelligence in Engineering, 2010
ISBN 978-3-642-15219-1

Vol. 314. Lorenzo Magnani, Walter Carnielli, and Claudio Pizzi (Eds.)
Model-Based Reasoning in Science and Technology, 2010
ISBN 978-3-642-15222-1

Vol. 315. Mohammad Essaaidi, Michele Malgeri, and Costin Badica (Eds.)
Intelligent Distributed Computing IV, 2010
ISBN 978-3-642-15210-8

Vol. 316. Philipp Wolfrum
Information Routing, Correspondence Finding, and Object Recognition in the Brain, 2010
ISBN 978-3-642-15253-5

Vol. 317. Roger Lee (Ed.)
Computer and Information Science 2010
ISBN 978-3-642-15404-1

Vol. 318. Oscar Castillo, Janusz Kacprzyk, and Witold Pedrycz (Eds.)
Soft Computing for Intelligent Control and Mobile Robotics, 2010
ISBN 978-3-642-15533-8

Vol. 319. Takayuki Ito, Minjie Zhang, Valentin Robu, Shaheen Fatima, Tokuro Matsuo, and Hirofumi Yamaki (Eds.)
Innovations in Agent-Based Complex Automated Negotiations, 2010
ISBN 978-3-642-15611-3

Vol. 320. xxx

Vol. 321. Dimitri Plemenos and Georgios Miaoulis (Eds.)
Intelligent Computer Graphics 2010
ISBN 978-3-642-15689-2

Vol. 322. Bruno Baruaque and Emilio Corchado (Eds.)
Fusion Methods for Unsupervised Learning Ensembles, 2010
ISBN 978-3-642-16204-6

Vol. 323. Yingxu Wang, Du Zhang, and Witold Kinsner (Eds.)
Advances in Cognitive Informatics, 2010
ISBN 978-3-642-16082-0

Vol. 324. Alessandro Soro, Vargiu Eloisa, Giuliano Armano, and Gavino Paddeu (Eds.)
Information Retrieval and Mining in Distributed Environments, 2010
ISBN 978-3-642-16088-2

Vol. 325. Quan Bai and Naoki Fukuta (Eds.)
Advances in Practical Multi-Agent Systems, 2010
ISBN 978-3-642-16097-4

Vol. 326. Sheryl Brahmam and Lakhmi C. Jain (Eds.)
Advanced Computational Intelligence Paradigms in Healthcare 5, 2010
ISBN 978-3-642-16094-3

Vol. 327. Slawomir Wiak and Ewa Napieralska-Juszczak (Eds.)
Computational Methods for the Innovative Design of Electrical Devices, 2010
ISBN 978-3-642-16224-4

Vol. 328. Raoul Huys and Viktor K. Jirsa (Eds.)
Nonlinear Dynamics in Human Behavior, 2010
ISBN 978-3-642-16261-9

Vol. 329. Santi Caballé, Fatos Xhafa, and Ajith Abraham (Eds.)
Intelligent Networking, Collaborative Systems and Applications, 2010
ISBN 978-3-642-16792-8

Vol. 330. Steffen Rendle
Context-Aware Ranking with Factorization Models, 2010
ISBN 978-3-642-16897-0

Vol. 331. Athena Vakali and Lakhmi C. Jain (Eds.)
New Directions in Web Data Management I, 2011
ISBN 978-3-642-17550-3

Vol. 332. Jianguo Zhang, Ling Shao, Lei Zhang, and Graeme A. Jones (Eds.)
Intelligent Video Event Analysis and Understanding, 2011
ISBN 978-3-642-17553-4

Vol. 333. Fedja Hadzic, Henry Tan, and Tharam S. Dillon
Mining of Data with Complex Structures, 2011
ISBN 978-3-642-17556-5

Vol. 334. Álvaro Herrero and Emilio Corchado
Mobile Hybrid Intrusion Detection, 2011
ISBN 978-3-642-18298-3

Álvaro Herrero and Emilio Corchado

Mobile Hybrid Intrusion Detection

The MOVICAB-IDS System

 Springer

Dr. Álvaro Herrero

University of Burgos

Civil Engineering Department Polytechnic School

Francisco de Vittoria s/n

09006 Burgos

Spain

E-mail: ahcosio@ubu.es

Prof. Dr. Emilio Corchado

University of Salamanca

Departamento de Informática y Automática

Facultad de Biología

Plaza de la Merced s/n

37008 Salamanca

Spain

E-mail: escorchado@usal.es

ISBN 978-3-642-18298-3

e-ISBN 978-3-642-18299-0

DOI 10.1007/978-3-642-18299-0

Studies in Computational Intelligence

ISSN 1860-949X

© 2011 Springer-Verlag Berlin Heidelberg

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typeset & Cover Design: Scientific Publishing Services Pvt. Ltd., Chennai, India.

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

Contents

Abbreviation.....	VII
Preface.....	IX
1 Introduction.....	1
2 Visualisation, Artificial Intelligence, and Security.....	3
2.1 Computer System Security	3
2.2 Intrusion Detection Systems	8
2.2.1 A General Architecture for ID.....	10
2.2.2 IDS Taxonomy	11
2.3 Visualisation for Network Security	13
2.4 Visualisation Techniques	15
2.5 Artificial Neural Networks	18
2.5.1 Artificial Neuron	19
2.5.2 Learning Algorithms	19
2.5.3 Hebbian Learning.....	21
2.5.4 Anti-Hebbian Learning.....	22
2.5.5 Competitive Learning.....	22
2.5.6 Principal Component Analysis	23
2.5.7 Oja's Weighted Subspace Algorithm.....	25
2.5.8 Negative Feedback Network	26
2.5.9 Nonlinear Principal Component Analysis	27
2.5.10 Exploratory Projection Pursuit	28
2.5.11 The Exploratory Projection Pursuit Network	29
2.5.12 Cooperative Maximum Likelihood Hebbian Learning.....	30
2.5.13 Self-Organizing Map.....	31
2.5.14 Curvilinear Component Analysis	32
2.6 Agents and Multiagent Systems	33
2.6.1 Agent Taxonomy	35
2.6.2 Agent Architecture	36
2.7 Case-Based Reasoning	36
3 Previous Work on NID	41
3.1 Overview of Techniques for NID.....	41
3.2 Visualisation.....	43
3.2.1 Visualisation Techniques	44
3.2.2 Visualised Data	55

3.3	Agents and Multiagent Systems	59
3.4	Novelties of the Proposed IDS	66
4	A Novel Hybrid IDS	71
4.1	Target Attacks	71
4.1.1	SNMP Attacks	74
4.2	System Overview	75
4.2.1	Network Traffic Capture and Selection	77
4.2.2	Data Segmentation	78
4.2.3	Data Analysis	80
4.2.4	Visualisation	80
4.3	Multiagent System	81
4.3.1	Methodology	81
4.3.2	Sniffer	83
4.3.3	Pre-processor	84
4.3.4	Analyzer	84
4.3.5	ConfigurationManager	87
4.3.6	Coordinator	87
4.3.7	Visualizer	89
5	Experiments and Results	91
5.1	GICAP-IDS Dataset	91
5.1.1	Dataset Description	92
5.1.2	Results	94
5.2	DARPA Dataset	102
5.2.1	Dataset Description	102
5.2.2	Results	102
6	Testing and Validation.....	105
6.1	Mutation Testing Technique	106
6.1.1	Mutating a Sample Dataset	107
6.1.2	Mutating Segments	113
6.2	Comparison with Other Projection Models	115
6.2.1	Principal Component Analysis	115
6.2.2	Curvilinear Component Analysis	117
6.2.3	Self-Organizing Map	118
7	Discussion and Conclusions	123
7.1	Discussion	123
7.2	Conclusions	125
7.3	Future Work	128
	References.....	129

Abbreviations

<i>AI</i>	Artificial Intelligence.
<i>ANN</i>	Artificial Neural Network.
<i>BDI</i>	Belief, Desire and Intention.
<i>CBR</i>	Case-Based Reasoning.
<i>CCA</i>	Curvilinear Component Analysis.
<i>CMLHL</i>	Cooperative Maximum-Likelihood Hebbian Learning.
<i>EPP</i>	Exploratory Projection Pursuit.
<i>HIDS</i>	Host-Based Intrusion Detection System.
<i>ID</i>	Intrusion Detection.
<i>IDS</i>	Intrusion Detection System.
<i>MAS</i>	Multiagent System.
<i>MIB</i>	Management Information Base.
<i>MLHL</i>	Maximum-Likelihood Hebbian Learning.
<i>NFN</i>	Negative Feedback Network.
<i>NID</i>	Network-Based Intrusion Detection.
<i>NIDS</i>	Network-Based Intrusion Detection System.
<i>PCA</i>	Principal Component Analysis.
<i>SNMP</i>	Simple Network Management Protocol.
<i>SOM</i>	Self-Organizing Map

Preface

This monograph gathers research efforts performed over a period of about five years and comprises works on network-based Intrusion Detection (ID) that is grounded on visualisation and hybrid Artificial Intelligence (AI). It has led to the design of MOVICAB-IDS (MOBILE VISUALISATION CONNECTIONIST AGENT-BASED IDS), a novel Intrusion Detection System (IDS), which is comprehensively described in this book.

This novel IDS combines different AI paradigms to visualise network traffic for ID at packet level. It is based on a dynamic Multiagent System (MAS), which integrates an unsupervised neural projection model and the Case-Based Reasoning (CBR) paradigm through the use of deliberative agents that are capable of learning and evolving with the environment. The proposed IDS applies a neural projection model to extract interesting projections of a traffic dataset and to display them through a mobile visualisation interface. As a result of depicting each simple packet and preserving the temporal context, MOVICAB-IDS provides security personnel with a synthetic, intuitive snapshot of network traffic and protocol interactions. This visualisation interface supports the straightforward detection of anomalous situations and their subsequent identification. Additionally, it helps ascertain the internal structure and the behaviour of the traffic data, thereby improving supervision of network activity.

The performance of MOVICAB-IDS was tested in different domains which entailed several attacks and anomalous situations and was further verified through a two-fold analysis. The proposed IDS was validated with a novel mutation-based testing method especially developed for that purpose, and the projections of its underlying neural model were compared with those obtained with some other projection models.

The monograph subsumes research results of the authors, a large part of which comes from Álvaro Herrero's PhD dissertation prepared at the University of Burgos (Spain) under the supervision of Dr. Emilio Corchado.

May 2010

Álvaro Herrero and Emilio Corchado
Burgos and Salamanca
Spain