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 Baruque 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 Brahnam 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 1, 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 Informáca y Automtica
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

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

Abbreviations

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