

Computer Science and Communications Research Unit

CSC Activity Report, 2010

Computer Science and Communications Research Unit

CSC Activity Report, 2010

Keywords:

Activity Report, University of Luxembourg, Computer Science and
Communications Research Unit, UL, CSC, \LaTeX .

Computer Science and Communications Research Unit, CSC Activity Report, 2010

Address:

Computer Science & Communication (CSC) Research Unit
University of Luxembourg
Faculty of Science, Technology and Communication
6, rue Richard Coudenhove-Kalergi
L-1359 Luxembourg
Luxembourg

Administrative Contact:

Isabelle Glemot-Schroeder and Fabienne Schmitz
Email: csc@uni.lu

<http://csc.uni.lu>

Editors:	Grégoire Danoy and Sébastien Varrette
Release date:	2010
Category:	1 (public)
Document Version:	Final v0.1 – SVN <i>Rev</i>
	Compiled time: 2011-11-30 19:49
Comments:	This report has been written using \LaTeX on the basis of the template [©] designed by Sebastien Varrette.

Preface

You will find in this report the progress and activities made by the **Computer Science & Communications (CSC)** research unit in 2010.

2010 has been the year of consolidation for CSC activities. We have been extremely active in helping the interdisciplinary center in security and trust (SnT) in its development. Three of CSC professors, i.e. Prof. Thomas Engel, Prof. Yves le Traon and Prof. Peter Ryan even created the first 3 laboratories of the SnT.

CSC has also been extremely fruitful in graduating PhD students. Indeed more than 20 PhD students received the title of Dr of the University of Luxembourg, speciality Computer Science this year. We also improved in 2010 the organization of CSC doctoral activities by appointing Prof. Raymond Bisdorff as head of the CSC doctoral school. Many activities including technical and non technical training have been organized in this context. Support has also been granted for the participation of our students to summer doctoral schools.

We aim for 2011 to increase the CSC activity in terms of bioinformatics, in particular to reinforce our collaboration with the Luxembourg Centre in Systems Biology (LCSB). Additionally a professorship position in embedded systems will be filled in order to strengthen our software engineering laboratory (LASSY) and related teaching activities (MICS).

We would like to thank the readers for their interest in our activity and invite them to visit our website (<http://csc.uni.lu>) but also to not hesitate to contact us for further information and potential cooperation.

*Prof. Dr. Pascal Bouvry,
Luxembourg, September 15, 2011*

Contents

1	The Computer Science & Communications (CSC) Research Unit	1
2	Executive Summary	3
2.1	Academic Staff Overview	4
2.2	Main activities in 2010	5
2.3	CSC Budget in 2010	6
3	CSC Laboratories	7
3.1	Laboratory for Advanced Software Systems	7
3.2	Laboratory of Algorithmics, Cryptology and Security	8
3.3	Communicative Systems Laboratory	9
3.4	Interdisciplinary Laboratory for Intelligent and Adaptive Systems	11
4	Projects and Grants in 2010	13
4.1	Research projects	22
4.1.1	European funding projects	22
4.1.2	FNR Projects	27
4.1.3	UL Projects	43
4.1.4	Other miscellaneous projects	56

4.2	Grants	67
4.2.1	AFR	67
4.2.2	Workshop & Conferences (FNR Accompanying Measures)	97
5	CSC Representation	99
5.1	Conferences	99
5.2	PC and other memberships	101
5.3	Doctoral board	109
5.4	Guests	111
5.5	Visits and other representation activities	113
5.6	Research meeting	115
5.6.1	ILIAS	115
5.6.2	LASSY	115
5.6.3	SaToSS Research Meeting	115
6	CSC Software	117
6.1	GreenCloud	117
6.2	OVINS	117
6.3	VehILux	117
6.4	SHARC	118
6.5	An Implementation of Basic Argumentation Components - ArguLab 0.2	118
6.6	Adaptive High-Interaction Honeypot Alternative (AHA)	118
6.7	MiCS Management System	118
6.8	bagit	119
6.9	Visual Contract Builder	119
6.10	Model Decomposer	119
7	CSC Publications in 2010	121
7.1	Books	121

7.2	Book Chapters	122
7.3	Book Chapters	124
7.4	International journals	124
7.5	Conferences Articles	127
7.6	PhD Thesis	146
7.7	Internal Reports	146
7.8	Proceedings	147
	Appendix	149
	A Acronyms used	149

The Computer Science & Communications (CSC) Research Unit

The **Computer Science & Communications (CSC)** research unit is part of the **University of Luxembourg** with the primary mission to conduct fundamental and applied research in the area of computer, communication and information sciences.

The goal is to push forward the scientific frontiers of these fields. Additionally, CSC provide support for the educational tasks at the academic and professional Bachelor and Master levels as well as for the PhD program.

The CSC Research Unit is divided into four laboratories:

1. **Communicative Systems Laboratory (ComSys)**
2. **Interdisciplinary Laboratory for Intelligent and Adaptive Systems (IL-
IAS)**
3. **Laboratory of Algorithmics, Cryptology and Security (LACS)**
4. **Laboratory for Advanced Software Systems (LASSY)**

Three laboratories of the interdisciplinary centre in security, reliability and trust (SnT) are also headed by CSC professors.

2 The Computer Science & Communications (CSC) Research Unit

CSC works intensively towards the University priorities in Security, Reliability and Trust as well as Systems Biomedicine. By providing a strong disciplinary knowledge in computer science, telecommunications and applied mathematics, CSC will serve as one of the fundamental bricks to enable interdisciplinary research through the University of Luxembourg's interdisciplinary centres.

CSC is currently the largest research unit of the University with a staff of more than 100 persons, including 23 professors, 10 scientific support staff members, 13 research associates, 13 post-doc researchers, 25 junior researchers, 13 PhD students (on projects), 3 technical support staff members, 4.75 full-time-equivalent administrative support positions.

Their research fields range from the investigation of the theoretical foundations to the development of interdisciplinary applications.

CSC decisions are taken by the chorus of professors. As described in Figure 1.1, the head of the research unit is helped by a quality manager, a facility manager (handled by the scientific facilitator) and the heads of labs in order to prepare the decision options and the reporting of the CSC. Each lab has its own budget line and a set of support resources.

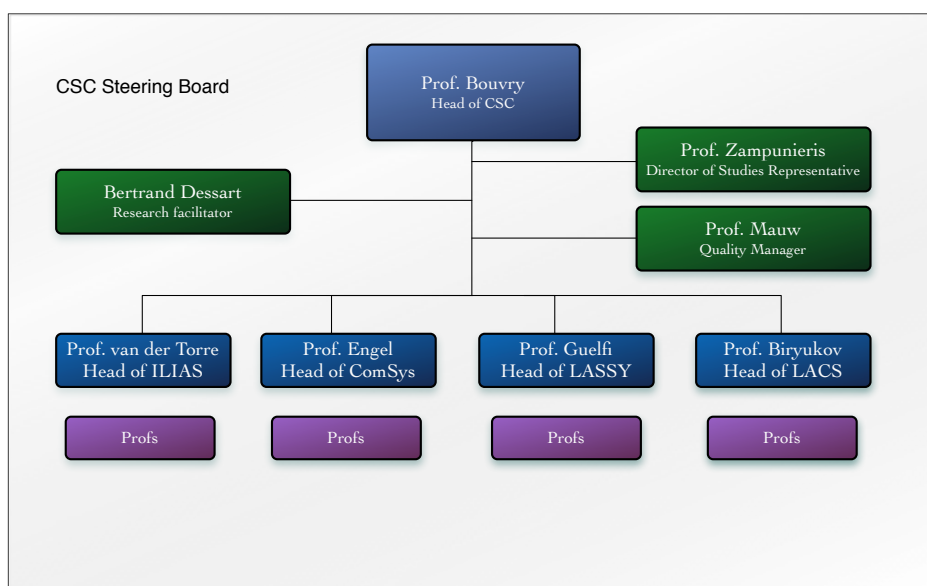


Figure 1.1: CSC Organisation

Executive Summary

The **Computer Science & Communications (CSC)** research unit, includes a staff of 105 persons end of 2010. Currently, we instruct more than 200 students at Bachelor and Master levels (Master in Information and Computer Science and Master in Security Management), and encourage them through close supervision and advice. For the professional branches, we want to bridge the gap between theory and practice, whereas for the academic branches, we foster on a problem-oriented understanding of the theoretical foundations of computer science. CSC is also active in developing the University priorities in Security, Reliability and Trust as well as System Biomedicine. By providing a strong disciplinary knowledge in computer science, telecommunications and applied mathematics, CSC will serve as one of the fundamental bricks to enable interdisciplinary research through the UL interdisciplinary centers. CSC is currently the largest research unit of the university and is cooperating in a large set of international as well as regional projects.

In parallel, CSC is more and more active in the field of distributed grid computing with the aim to propose and/or join attractive academic projects in this area. In this context, CSC hosts and manages several High Performance Computing (**HPC**) facilities, in particular the **chaos** cluster (featuring 67 nodes, 656 computing cores for a theoretical peak performance $R_{\text{peak}} = 6$ TFlops) and the **lux5000** cluster (22 nodes, 176 computing cores for a theoretical peak performance $R_{\text{peak}} = 1,4$ TFlops). Whereas the first cluster is used internally for all university research units (see <http://cluster1a.uni.lu>), the second one is part of the **Grid5000** project, an

experimental grid distributed among several sites (mainly in France) for research in large-scale parallel and distributed systems. Currently, all HPC facilities are hosted between two server rooms in the Kirchberg campus site. In 2011, it is planned an extension of the HPC capacities (both in terms of computing and storage) thanks to the disposal of a new server room in the first building of the Belval campus.

2.1 Academic Staff Overview

- Jean-Claude Asselborn, professor
- Alex Biryukov, associate professor, head of LACS
- Raymond Bisdorff, professor
- Pascal Bouvry, professor, head of CSC and ILIAS
- Jean-Sébastien Coron, associate professor
- Dov Gabbay, guest professor
- Theo Duhautpas, senior lecturer
- Thomas Engel, professor, head of ComSys
- Nicolas Guelfi, professor, head of LASSY
- Pierre Kelsen, professor
- Franck Leprévost*, professor, vice rector
- Yves Le Traon, professor
- Sjouke Mauw, professor
- Volker Müller, associate professor
- Björn Ottersten, professor
- Steffen Rothkugel, associate professor
- Peter Ryan, professor
- Jürgen Sachau, professor
- Christoph Schommer, associate professor
- Ulrich Sorger, professor
- Bernard Steenis, associate professor

- Leon van der Torre, professor
- Denis Zampuniéris, professor

2.2 Main activities in 2010

The following local events have been organized during 2010:

- **BNAIC 2010**, the 22nd Benelux Conference on Artificial Intelligence (October 25-26) was organised together with the CRP Henri Tudor in Luxembourg Kirchberg.
- **Early Symmetric Crypto (ESC)** seminar (January 11-15) was organized in Remich, Luxembourg.
- **Robocafé**: A successful public outreach event in the context of the Researchers'Night 2010 (September 24), where talks and a show of Nao robots were proposed, as well as a crypto for kids workshop.
- **Special AI Lecture Series, Vol. III - Data Mining Applications**, October 26-Dec 7, 2010.

CSC also participates at the organisation of many international conferences and workshops.

CSC is having strong partnerships with the other Luxembourgian research centres through the co-supervision of PhD students, co-organised projects and teaching activities.

In 2010, 21 PhD students successfully defended their PhD thesis at the CSC: Maria Biryukov, Nicolas Boizot, Patrice Caire, Alfredo Capozucca, Markus Esch, Daniel Fisher, Raphael Frank, Barbara Gallina, Patrick Gratz, Thomas Icart, Thomasz Ignac, Sascha Kaufmann, Dimitry Khovratovich, Michael Noll, Marek Ostaszewski, Apivadee Piyatumrong, Julien Schleich, Kenneth Sebesta, Dagmara Spiewak, Eugen Staab, Michael Stieghahn.

CSC members are taking active part in various boards country-wide: executive direction of ERCIM, direction of RESTENA, chairman of Luxcloud board, treasurer of CRP Tudor, vice-rectorate for international affairs and special projects of the University of Luxembourg, chairman of Luxconnect SA, member of LUXTRUST administration board, members of the SnT interim steering board and SnT faculty boards, representative of Luxembourg in the COST ICT DG, experts for EU and national projects.

CSC is active in various networks and projects: International, EU (FP, Eureka, COST), regional (UGR) and local (FNR) networks and projects.

CSC participates to various ERCIM workgroups - the European Research Consortium for Informatics and Mathematics through the FNR.

CSC also participated to the open source community by several contributions:

- [Green Cloud](#)
- [OVNIS](#)
- [VehILux](#)
- [SHARC](#)
- [ArguLab 0.2](#)
- [Adaptive High-Interaction Honeypot Alternative \(AHA\)](#)

CSC in 2010 produced 1 book, 5 book chapters and in terms of international peer-reviewed publications: 30 journal articles and 157 conference and workshop proceedings (see chapter 7 page 121 for more details). The full list of CSC publications is available [here](#).

2.3 CSC Budget in 2010

The following table describes the marginal expenses of CSC in terms of structural funding and UL projects. The main cost corresponds to the salaries of the structural positions (professors, research assistants, assistants, administrative and support staff), expenses related to the buildings and some of the operating expenses (e.g. phone bills, electricity, etc) are covered by the structural UL budget.

Details on CSC external funding can be found in the [SnT Annual Report](#).

Lab structural funding	825,345€
UL Research Projects	782,663€
Total	1,608,008€

Table 2.1: CSC Internal Budget

CSC Laboratories

3.1 Laboratory for Advanced Software Systems

Laboratory of Advanced Software Systems	
Acronym	LASSY
Reference	F1R-CSC-LAB-05LASS
Head	Prof. Dr. Nicolas Guelfi

Scientific Board:

Nicolas Guelfi, Pierre Kelsen, Yves Le Traon

Domain(s):

- dependability
- e-learning
- hardware/software co-design
- model driven engineering
- proactive computing
- security
- software engineering

- software product lines
- technical systems modeling and simulation
- testing
- verification

Objectives:

The Laboratory for Advanced Software Systems (LASSY) is conducting research on methods and tools for mastering the development of complex software systems. It focuses on the following application domains: industry-critical systems, e-learning systems, web-based distributed systems. The current research objectives are the following ones:

- To develop new engineering processes,
- To investigate modeling languages,
- To use mathematical theories in the definition and verification of new software engineering artifacts,
- To address dependability attributes (availability, reliability, safety, confidentiality, integrity and maintainability) throughout all the development life cycle,
- To assist in the development and in the use of e-learning tools,
- To study verification and validation techniques.

3.2 Laboratory of Algorithmics, Cryptology and Security

Laboratory of Algorithmics, Cryptology and Security	
Acronym	LACS
Reference	F1R-CSC-LAB-F01L0204
Head	Prof. Dr. Alex Biryukov

Scientific Board:

Jean-Claude Asselborn, Jean-Sébastien Coron, Franck Leprévost, Sjouke Mauw, Volker Müller, Peter Ryan

Domain(s):

- Cryptography Information and Network Security
- Information Security Management
- Embedded Systems Security
- Side-Channel Analysis and Security of Implementations
- Algorithmic Number Theory

Objectives:

In recent years, information technology has expanded to encompass most facets of our daily lives—at work, at school, at home for leisure or learning, and on the move—and it is reaching ever-widening segments of our society. The Internet, e-mail, mobile phones, etc. are already standard channels for the information society to communicate, gain access to new multimedia services, do business, or learn new skills. The recent “digital revolution” and widespread access to telecommunication networks have enabled the emergence of e-commerce and e-government. This proliferation of digital communication and the transition of social interactions into the cyberspace have raised new concerns in terms of security and trust, like: confidentiality, privacy and anonymity, data integrity, protection of intellectual property and digital rights management, threats of corporate espionage, and surveillance systems (such as Echelon), etc. These issues are interdisciplinary in their essence, drawing from several fields: algorithmic number theory, cryptography, network security, signal processing, security of protocols, side-channel analysis, software engineering, legal issues, and many more.

3.3 Communicative Systems Laboratory

Communicative Systems Laboratory	
Acronym	ComSys
Reference	F1R-CSC-LAB-05COMS
Head	Prof. Dr. Thomas Engel

Scientific Board:

Pascal Bouvry, Thomas Engel, Steffen Rothkugel, Sjouke Mauw, Théo Duhautpas

Domain(s):

- Information Transmission

- Wireless Communication Systems
- Security Protocols
- Trust Models
- Middleware
- Parallel and Distributed Systems
- Cloud, Grid and Peer-to-Peer Computing
- Management and Mining of Data

Objectives:

The Communicative Systems Laboratory (ComSys) is part of the Computer Science and Communication Research Unit and focuses on state of the art research in digital communications. Embracing the end-to-end arguments in system design, ComSys focuses on integrated research in the areas of Information Transfer and Communicating Systems. Information Transfer is concerned with information transmission over potentially complex channels and networks. Communicating Systems in turn are the composition of multiple distributed entities employing communication networks to collaboratively achieve a common goal. ComSys has strong technical and personal facilities to improve existing and develop new solutions in the following research topics.

The ComSys research fields will have a strong impact on the 21st century. The rapidly growing demand for information exchange in people's daily lives requires technologies like ubiquitous and pervasive computing to meet the expectations of the information society and novel adaptive concepts tackling the continuing data challenges. The resulting problems have already been a key enabler for some industrial and governmental founded projects at national and European level. Current research projects propagate technologies for:

- Hybrid Wireless Networks
- Green Cloud Computing
- Information Dissemination in Ad-Hoc Networks
- Mobile Communication
- Mobile Learning
- Network Traffic Analysis and Protection

3.4 Interdisciplinary Laboratory for Intelligent and Adaptive Systems 11

- Network Traffic Management and Coordination
- Secure Satellite Communication
- Secure Wireless MANETs

3.4 Interdisciplinary Laboratory for Intelligent and Adaptive Systems

Interdisciplinary Lab on Intelligent and Adaptive Systems	
Acronym	ILIAS
Reference	F1R-CSC-LAB-05ILIA
Head	Prof. Dr. Leon van der Torre

Scientific Board:

Pascal Bouvry, Raymond Bisdorff, Christoph Schommer, Ulrich Sorger, Leon van der Torre

Domain(s):

- Optimization
- Parallel computing
- Bio-inspired computing
- Algorithmic decision theory
- Data mining and knowledge discovery
- Information theory and uncertain inference
- Knowledge representation and applied logics
- Normative multi-agent systems
- Cognitive agents/robots

Objectives:

ILIAS is a cross-disciplinary research group combining expertise from computer science, operational research, information theory, mathematics, and logic. The overarching subject is information processing in complex and dynamic environments given limited resources and incomplete or uncertain

knowledge. It investigates the theoretical foundations and the algorithmic realization of systems performing complex problem solving with a high degree of autonomy, i.e. intelligent systems, and exploiting learning to deal with opaque and dynamic contexts, i.e. adaptive systems.

Projects and Grants in 2010

This chapter lists the research projects running during 2010 together with the grants obtained (typically to organize scientific conferences via the FNR accompanying measures AM3).

This chapter is structured to summarize:

1. European funding project (FP7, ERCIM etc.) – see §4.1.1
2. FNR CORE projects – see §4.1.2
3. UL projects – see §4.1.3
4. Other miscellaneous projects (French ANR, Grant agreement for research, development, and innovation etc.) – see §4.1.4
5. Grants obtained (AFR, FNR AM3 etc.) – see §4.2.

The following tables summarize the projects operated in CSC for the year 2010.

European projects

Lab	Acronym	Title	PI	Funding	Duration
COMSYS	ceFIMS Ref: p.22	SceFIMS-Coordination of the European Future Internet forum of Member States	Prof. Dr. Thomas Engel	EC - FP7 UL budget: 35000€.	01/09/2010 – 31/05/2013
	SECRICOM Ref: p.23	Seamless Communication for Crisis Management	Prof. Dr. Thomas Engel	EC - FP7 European Commission. UL budget: 304.625€.	01/09/2008 – 31/05/2012
ILIAS	WiSafeCar Ref: p.24	Wireless traffic Safety network between Cars	Pekka Elo- ranta (Mo- bisoft, Fin- land)	EUREKA - CELTIC, 300000€	01/07/2009 – 31/12/2011

FNR projects

Lab	Acronym	Title	PI	Funding	Duration
LACS	ATREES Ref: p.27	Attack Trees	Prof. Dr. Sjouke Mauw	FNR-CORE, 299000€	01/04/2009 – 31/03/2012
	CRYPTOSECC Ref: p.29	Cryptography and Information Security in the Real World	Dr. Jean-Sébastien Coron	FNR-CORE, 272000€	01/10/2010 – 30/09/2013
	SeRTVS Ref: p.30	Secure, Reliable and Trustworthy Voting Systems	Prof. Dr. Peter Ryan	FNR-Core, 333000€ FNR-AFR, 216216€ IMT Luca, 130000€ University of Melbourne, 60000€ UL, 268596€	01/02/2010 – 01/02/2013
LASSY	MaRCo Ref: p.33	Managing Regulatory Compliance: a Business-Centred Approach	Prof. Dr. Pierre Kelsen	FNR-CORE, 749K €	01/05/2010 – 30/04/2013
	MOVERE Ref: p.31	Model-Driven Validation and Verification of Resilient Software Systems	Prof. Nicolas Guelfi	FNR-CORE, 265 000€	1/5/2010 – 30/4/2013
	SETER Ref: p.34	Security TESting for Resilient systems	Prof. Nicolas Guelfi	FNR-CORE, 438,300.00 €	01/05/2009 – 30/04/2012
ILIAS	S-GAMES Ref: p.39	Security Games	Prof. Dr. Leon van der Torre	FNR-CORE, 314000€	01/04/2009 – 31/03/2012
	DYNARG Ref: p.41	The Dynamics of Argumentation	Prof. Dr. Leon van der Torre	FNR-INTER/CNRS	01/10/2009 – 31/09/2012
	GreenIT Ref: p.37	EnerGy-efficient REsourcE Allocation in AutonomIc Cloud CompuTing	Prof. Dr. Pascal Bouvry	FNR-CORE, 432000€	1/01/2010 – 31/12/2012
	TITAN Ref: p.36	Trust-assurance for critical infrastructures in multi-agents environments	Dr. Benjamin Gateau	FNR-CORE, 108000€	1/01/2009 – 31/12/2010

AFR projects

Lab	Acronym	Title	PI	Funding	Duration
COMSYS	RDFGraTra Ref: p.94	Implementation of Formally Well-Founded Graph Transformations on the Resource Description Framework with Applications to Domain-Specific Modelling Languages	Prof. Dr. Thomas Engel	FNR - AFR PostDoc - 52817€	2010-2011
	WiNSEOM Ref: p.95	Energy Optimization and Monitoring in Wireless Mesh Sensor Networks	Prof. Dr. Thomas Engel	FNR - AFR PhD - 36042 €/year	01/09/2010 - 31/08/2013
LACS	EPRIV-MAA Ref: p.67	A Formal Approach to Enforced Privacy: Modelling, Analysis and Applications	Prof. Dr. Sjouke Mauw	FNR-AFR, 105222€	01/12/2009-30/11/2012
	GMASec Ref: p.68	Games for Modelling and Analysis of Security	Prof. Dr. Sjouke Mauw	FNR-AFR, 105223,44€	01/11/2009-31/10/2012
	CRHF Ref: p.71	Cryptanalysis of Hash Functions	Prof. Dr. Alex Biryukov	FNR-AFR PhD, 109€ per year	01/05/2007 - 28/02/2011
	SADT Ref: p.69	Security Analysis Through Attack-Defense Trees	Prof. Dr. Sjouke Mauw	FNR-AFR, 106476€	01/01/2010-31/12/2012
	SECLOC Ref: p.74	Secure and Private Location Proofs: Architecture and Design for Location-Based Services	Prof. Dr. Sjouke Mauw	FNR-AFR PhD, 109137€	01/08/2010-31/07/2013
	SHARC Ref: p.73	Analysis of the SHA-3 Remaining Candidates	Prof. Dr. Alex Biryukov	FNR-AFR Postdoc, 102,620€	15/10/2010 - 14/10/2012
	SPIM Ref: p.70	Security Protocols in Identity Management	Prof. Dr. Sjouke Mauw	BFR, FNR-AFR, 18000€+ 70984€+ 36379€	01/10/2007-30/11/2011
	RKCTM Ref: p.72	Refining Key Components in Trust Models	Prof. Dr. Sjouke Mauw	FNR-AFR Postdoc, 50360€ per year	01/01/2009-31/07/2010

AFR projects (cont.)

Lab	Acronym	Title	PI	Funding	Duration
LASSY	ENRDEM Ref: p.76	Expressing Non-Functional Requirements in Declarative Executable Models	Prof.Dr.Pierre Kelsen	FNR, BFR/AFR ,	01/01/2008 - 31/05/2010
	PRISMA Ref: p.77	PRISMA : a Process for Requirements Identification, Specification and Machine-supported Analysis, targeting Transactional Models seen under a Product Line perspective	Prof. Dr. Nicolas Guelfi	N/A	16/03/2006 – 15/03/2010
	SPEM Ref: p.78	Selected Problems in Executable Modeling	Prof. Dr. Pierre Kelsen	FNR-AFR PhD	15/11/2009 – 15/11/2012

AFR projects (cont.)

Lab	Acronym	Title	PI	Funding	Duration
ILIAS	ULFAUC Ref: p.91	Towards a unified logical framework for action, uncertainty, and causality	Prof. Dr. Leon van der Torre	FNR-AFR-Postdoc	01/09/2008 – 31/08/2010
	LCNMAS Ref: p.92	Logic and Communication in Normative Multi-Agent Systems	Prof. Dr. Leon van der Torre	FNR-AFR-Postdoc	01/03/2009 – 28/02/2011
	TMAHN Ref: p.81	Trust Management for Ad-Hoc Networks	Prof. Dr. Pascal Bouvry	FNR - AFR PhD	01/02/2007 – 31/01/2011
	CIDC Ref: p.83	Confidentiality, Integrity issues in distributed computations	Prof. Dr. Pascal Bouvry	FNR - AFR PhD	01/01/2010 – 31/12/2012
	COPSCG Ref: p.85	Combinatorial optimization on P2P systems and computational grids	Prof. Pascal Bouvry	FNR - AFR PhD	01/09/2007 - 31/10/2011
	RSDG Ref: p.86	Robust Scheduling on Desktop Grids	Prof. Dr. Pascal Bouvry	FNR - AFR PostDoc	01/09/2009 – 31/08/2011
	WiCaN Ref: p.87	Efficient data transfer in vehicle2vehicle wireless communication networks, using distributed algorithms based on collective intelligence such as ant colonies.	Prof. Dr. Pascal Bouvry	FNR - AFR PostDoc	15/10/2009 – 14/10/2011
	EPOC Ref: p.88	Energy-Performance Optimization of the Cloud	Prof. Dr. Pascal Bouvry	FNR - AFR PhD 108125.58 €.	01/09/2010 – 31/08/2013
	TIGRIS Ref: p.90	Risk Prediction Framework for Interdependent Systems using Graph Theory	Prof. Dr. Pascal Bouvry	FNR - AFR PhD	15/10/2009 – 15/10/2012
	R2MTO Ref: p.80	Reliable and robust management for telecommunication network with optimization techniques	Prof. Dr. Pascal Bouvry	FNR - AFR PhD	01/12/2008 – 30/11/2010

University of Luxembourg Internal project

Lab	Acronym	Title	PI	Funding	Duration
LACS	EPRIV Ref: p.43	A Formal Approach to Enforced Privacy in e-Services	Prof. Dr. Sjouke Mauw	UL, 254955€	01/05/2009 – 30/04/2012
	ESS Ref: p.45	Embedded Systems Security	Prof. Dr. Alex Biryukov, Prof. Dr. Jean-Sebastien Coron, Prof. Dr. Sjouke Mauw	UL, 499514€	01/10/2008 – 31/01/2012
	SECRYPT Ref: p.46	Security and Cryptography in the Real World	Prof. Dr. Jean-Sébastien Coron	UL, 950000 €	01/01/2007 – 31/08/2010
LASSY	AHEKFA Ref: p.47	Adaptive High-gain Extended Kalman Filter and Applications	Prof. Dr. Juergen Sachau	Junior Researcher contract, University of Luxembourg project: RAIP.	2006 – 2010
	BLAST Ref: p.49	Better e-Learning Assignments System Technology	Prof. Dr. Denis Zampuniéris	UL, 165000€	01/09/2010 – 31/08/2012
	MEDAL Ref: p.50	Model-Driven Engineering using a Declarative Behavioural Description Language	Prof. Dr. Pierre Kelsen	UL, 171K€	01/10/2008 – 30/09/2011
	RAID Ref: p.51	Resource Allocation in Delay and Disruption Tolerant Networks	Prof. Dr. Simin Najdm-Tehrani	UL	01/09/2007 – 01/09/2011
	VERITY Ref: p.52	VERification of fault-tolerant advanced Transactional distributed sYstems	Prof. Dr. Nicolas Guelfi	University of Luxembourg, 364257€	01/01/2008 – 31/03/2011
ILIAS	ICR Ref: p.54	Individual and Collective Reasoning	Prof. Dr. Leon van der Torre	UL-PHD	12/03/2008 – 12/03/2012
	AASTM Ref: p.53	Advanced Argumentation Techniques for Trust Management	Prof. Dr. Leon van der Torre	UL	01/05/2008 – 30/04/2012

Other misc projects

Lab	Acronym	Title	PI	Funding	Duration
COMSYS	MBITSRC Ref: p.58	Modelling of Business and IT Landscapes addressing Security, Risk and Compliance in a Real-World banking environment (PhD thesis)	Prof. Dr. Thomas Engel	Credit Suisse and FNR (128.50K€)	2005-2010
	EWSSAOP Ref: p.58	End-to-end Web Service Security in AspectOriented Programming	Prof. Dr. Thomas Engel	EPT (75K€)	2008 – 2011
	EPTV Ref: p.60	EPT Vehicular Networks	Prof. Dr. Thomas Engel	EPT - 2 298 K€	01/01/2010-31/12/2014
	FSTO Ref: p.61	Feasability Study for Topology Optimization	Prof. Dr. Thomas Engel	Ministry of Commerce - 40000 €	2010
	SMO-MLS Ref: p.61	Securing Mission Operations using Multi-Level Security	Prof. Dr. Thomas Engel	European Space Agency - 48800€ UL - 37077 €	01/11/2010 – 01/11/2013
	SOSSHIN Ref: p.62	Self Organizing Security Sensors in highly-distributed IP networks (PhD thesis)	Prof. Dr. Thomas Engel	SES-ASTRA and FNR - 45K€	2007 – 2011
	SUTMDNiBE Ref: p.63	Secure Usage and Trust of Mobile Devices in Networks for international banking environments (PhD thesis)	Prof. Dr. Thomas Engel	Dresdner Bank and FNR - 45K€	2005-2010
LACS	LEWIS Ref: p.65	Luxembourgish Early-Warning Analysis and Information Sharing System	Prof. Dr. Peter Ryan	Ministry of Economy - 70000€ UL, 29120€	01/10/2009 – 31/05/2010
	LASP Ref: p.65	Developing a Prototype of Location Assurance Service Provider	Prof. Dr. Sjouke Mauw	ESA 160000€, SnT 80000€	08/12/2010–07/12/2012
LASSY	SPLIT Ref: p.56	Combine Software Product Line and Aspect-Oriented Software Development	Prof. Dr. Nicolas Guelfi	UL/FNR, 41 000€	01/10/2009 – 30/09/2012

Accompanying measures (AM)

Lab	Acronym	Title	PI	Funding	Duration
LACS	ESC 2010 Ref: p.97	ESC 2010 - Early Symmetric Cryptography Workshop	Prof. Dr. Alex Biryukov	FNR-AM3, 8000€	11/01/2010 - 15/01/2010

4.1 Research projects

4.1.1 European funding projects

SceFIMS-Coordination of the European Future Internet forum of Member States	
Acronym	ceFIMS
Reference	To be defined
Head of Project	Prof. Dr. Thomas Engel
Funding	EC - FP7
	UL budget: 35000€.
Running Time	01/09/2010 – 31/05/2013

Members:

Thomas Engel, Latif Ladid

Domain(s):

IPv6, networking, support action

Partner(s):

- Waterford Institute of Technology, Ireland
- Nederlandse Organisatie voor Wetenschappelijk Onderzoek, Netherlands
- Nemzeti Kutatási Es Technológiai Hivatal, Hungary
- UMIC - Agência Para A Sociedade Do Conhecimento, Portugal
- Asociacion De Empresas De Electronica, Tecnologias De La Informacion Y Telecomunicaciones De Espana, Spain

Description:

The ceFIMS project addresses the problem of the fragmentation of ICT research between European Member States (MS). ceFIMS will leverage its knowledge of Member State-funded research to gain consensus about problems and approaches at the Member State level. ceFIMS will build on that consensus to promote alignment both across Member States and also between Member State and EC-funded ICT research. This will, consequently, unite better the European ICT research community and place European Future Internet (FI) research in a stronger position.

ceFIMS will produce a research roadmap to maximise synergies between EU and MS investments in FI research, establishing the basis for an ERA-NET+ on the Future Internet. An ERA-NET+ will provide the means to develop the EU's strong research position. Allied to this, a Public-Private Partner-

ship (PPP) will provide the means to transfer new knowledge into innovative products, with economic and social benefits for EU citizens. ceFIMS will increase awareness among Member States of the role that they can play in a Europe-wide FI PPP and how Member State initiatives and the PPP can be aligned to the maximum extent possible.

ceFIMS-Coordination of the European Future Internet forum of Member States-responds to Call 5 from the European Commission for European excellence in Trustworthy ICT. In particular, the Science and Technology objectives of ceFIMS are highly relevant to Objective ICT-2007.1.1 The Network of the Future.

Results: HASH(0x1008ada10)

Seamless Communication for Crisis Management	
Acronym	SECRICOM
Reference	F1R-CSC-PEU-08SECR
Head of Project	Prof. Dr. Thomas Engel
Funding	EC - FP7 European Commission. UL budget: 304.625€.
Running Time	01/09/2008 – 31/05/2012

Members:

Thomas Engel, Latif Ladid, Aurel Machalek

Domain(s):

Emergency services, critical infrastructure

Partner(s):

- QinetiQ Ltd., United Kingdom
- Ardaco, a.s., Slovakia
- Bumar Ltd, Poland
- NEXTEL S.A., Spain
- Infineon Technologies AG, Germany
- Institute of Informatics, Slovak Academy of Sciences, Slovakia
- Graz University of Technology, Austria
- Smartrends, s.r.o., Slovakia
- ITTI Sp. z o.o., Poland
- British Association of Public Safety Communication Officers, United Kingdom
- CEA LETI, France
- Hitachi Europe SAS, France

Description:

SECRICOM is proposed as a collaborative research project aiming at development of a reference security platform for EU crisis management operations with two essential ambitions: (A) Solve or mitigate problems of contemporary crisis communication infrastructures (Tetra, GSM, Citizen Band, IP) such as poor interoperability of specialized communication means, vulnerability against tapping and misuse, lack of possibilities to recover from failures, inability to use alternative data carrier and high deployment and operational costs. (B) Add new smart functions to existing services which will make the communication more effective and helpful for users. Smart functions will be provided by distributed IT systems based on an agents' infrastructure. Achieving these two project ambitions will allow creating a pervasive and trusted communication infrastructure fulfilling requirements of crisis management users and ready for immediate application.

More information: <http://www.secricom.eu>

Results:

University of Luxembourg successfully organised and presented developed crises communication technology of SECRICOM project during the NATO CPC seminar and demonstration in Slovakia. We did the demonstration together with Civil Protection of Luxembourg. The project SECRICOM is after first review period marked as: "Excellent progress (the project has fully achieved its objectives and technical goals for the period or has even exceeded expectations)".

Wireless traffic Safety network between Cars	
Acronym	WiSafeCar
Reference	N/A
Head of Project	Pekka Eloranta (Mobisoft, Finland)
Funding	EUREKA - CELTIC, 300000€
Running Time	01/07/2009 – 31/12/2011

Members:

Pascal Bouvry, Grégoire Danoy, Yoann Pigné, Guillaume-Jean Herbiet, Patricia Ruiz.

Domain(s):

Vehicular Ad Hoc Networks, Secure Communications, Traffic Management, Accident Warning.

Partner(s):

- Mobisoft, Finland
- Finnish Meteorological Institute, Finland
- VTT, Finland
- Taipale Telematics, Finland
- Sunit, Finland
- Ubridge, South Korea
- CRP Henri Tudor
- Ubistream, Luxembourg

Description:

WiSafeCar aims to develop an effective service platform and advanced intelligent wireless traffic safety network between cars and infrastructure, with possibility to exploit vehicle based sensor and observation data in order to generate secure and reliable intelligent real-time services and service platform for vehicles.

Results:

Nowadays energy management is a key feature in many different fields, specially in mobile ad hoc networks where devices heavily rely on the battery life, thus, the network survival is absolutely related to the energy consumption of nodes. AEDB, a broadcasting algorithm that not only tries to reduce the network but also the device resources has been proposed in [185]. AEDB is an extension of EDB which is a distance based broadcasting and also energy aware. The new proposed scheme, AEDB, regulates the transmission power of the device in order to decrease the energy consumption with no detriment of the performance of the algorithm.

A fully distributed algorithm (SHARC: Sharper Heuristic for Assignment of Robust Communities) has been designed to discover subsets of densely connected users of a mobile ad hoc network, using social network analysis techniques (community detection).

This algorithm has later been improved to account for the reliability of the interconnection links (Saw-SHARC: Stability Aware SHARC) and to better manage the specificities of dynamic networks (SAND/SHARC: Stability and Network Dynamics over SHARC).

Those solutions have been tested two kind of scenarios :

- *mobile social networks*: where the generated reliable communities are used to favor social-based interactions between human users carrying

handheld communicating devices (smartphones, tablets, etc.)

- *vehicular ad hoc networks*; where the community structure is valuable for a more efficient and reliable propagation of safety messages between communicating vehicles, and can be also used to minimize the number of connections to the ITS (Intelligent Transportation System) core network.

The SHARC algorithm has been presented at the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoW-MoM) in June 2010.

The SAw-SHARC algorithm has been presented at the International Conference on Communication Networking (ICOIN) in January 2011.

The SAND/SHARC algorithm has been submitted to the International Conference on Distributed Computing Systems (ICDCS) on late 2010.

A complete review of the new techniques for social network analysis introduced by the SHARC family of algorithms as been submitted for publication as a chapter of the book "Social Networks: Computational Aspects and Mining", in the Series "Computer and Communication Networks", published by Springer.

Argument-based Contextual Defeasible Reasoning	
Acronym	CDL
Reference	ERCIM
Head of Project	Prof. Dr. Leon van der Torre
Funding	ERCIM
Running Time	20/09/2010 – 20/09/2011

Members:

Antonis Bikakis

Domain(s):

Defeasible argumentation, Formal models of context, Multi-context systems

Description:

Aim of the project is to extend existing approaches on reasoning with multiple contexts in domains characterized by imperfection and distribution of the available knowledge. Multi-context systems and defeasible argumentation constitute the underlying formal models of our approach. Potential application domains include ambient intelligence and social networks.

Results:

- We extended Contextual Defeasible Logic with a partial preference relation on the system contexts, which is modeled as a directed acyclic graph, and modified accordingly the argumentation model and the reasoning algorithms.
- We described four different variants of Contextual Defeasible Logic, integrating the notions of ambiguity propagation and team defeat, which are typical in nonmonotonic reasoning models.

The results were reported in a paper which has been accepted for LPNMR 2011.

4.1.2 FNR Projects

Attack Trees	
Acronym	ATREES
Reference	C08/IS/26
Head of Project	Prof. Dr. Sjouke Mauw
Funding	FNR-CORE, 299000€
Running Time	01/04/2009–31/03/2012

Members:

Sjouke Mauw, Barbara Kordy, Patrick Schweitzer, Saša Radomirović

Domain(s):

security, attack–defense trees, security assessment, formal methods

Partner(s):

- SnT
- Telindus, Luxembourg
- Sintef, Norway
- TXT e-solutions, Italy
- Cybernetica, Estonia

Description:

Security assessment of systems is a standard but suboptimal procedure due to its informal nature. While a formal approach would be desirable, but out of reach, a systematic approach would be beneficial and feasible.

Attack trees are a well-known methodology to describe the possible security weaknesses of a system. An attack tree basically consists of a description of an attacker's goals and their refinement into sub-goals. We believe that attack trees provide an ideal systematic approach for security assessment.

The objective of this project is to extend attack trees with defensive measures. Consequently, the attack-defense tree methodology will be developed and formalized, in order to provide a systematic, fully-fledged, and practical security assessment tool.

The project benefits from our contacts with several industrial and academic partners with whom we conduct case studies.

Results:

The formalism for attack-defense trees (ADTrees) has been developed, in particular different semantics for ADTrees have been introduced and analysed. An official publication 'Foundation of Attack-Defense Trees' ([74]) by Barbara Kordy, Sjouke Mauw, Saša Radomirović and Patrick Schweitzer, describing the corresponding results, has been accepted at FAST'2010.

Thanks to the cooperation between ATREES and GMASec projects, the relation between security assessment problem and game theory has been established. It resulted in a publication on equivalence between attack-defense trees under propositional semantics and two-player binary zero-sum extensive form games [179]. Currently, together with Marc Pouly from SnT, the ATREES team is working on comparing attack-defense trees language to known compilation languages like BDDs or sublanguages of PDAGs. It will allow us to use the well known results from AI in order to better understand the security assessment problem.

BK and PS, presented their work related to the project by giving five talks in Luxembourg, France and Italy. Moreover, contacts with several researchers working in attack trees area have been made, in 2010. Jan Willemson from Cybernetica (Estonia) and Per Hakon Meland from SINTEF (Norway) visited Barbara Kordy, Sjouke Mauw, Saša Radomirović and Patrick Schweitzer, and presented their work in the field at SaToSS research seminar. The presentations resulted in very interesting discussions on the attack-defense trees formalism and its applicability.

Finally, a research on several case studies has been conducted with our industrial and academic partners:

- *Attack-defense trees for penetration testing*, with Telindus Luxembourg,
- *How to change an RFID information*, with Shields project, SINTEF Norway and TXT Italy,

- *An attack–defense tree for an on-line auction* developed for the Trust in Digital Life Consortium.

Cryptography and Information Security in the Real World	
Acronym	CRYPTOSEC
Reference	F1R-CSC-PFN-09IS04
Head of Project	Dr. Jean-Sébastien Coron
Funding	FNR-CORE, 272000€
Running Time	01/10/2010 - 30/09/2013

Domain(s):

Cryptography, Information Security, Side-Channel Attacks

Description:

Cryptography is only one component of information security, but it is a crucial component. Without cryptography, it would be impossible to establish secure communications between users over insecure networks like the internet. In particular, public-key cryptography (invented by Diffie and Hellmann in 1974) enables to establish secure communications between users who have never met physically before. One can argue that companies like E-Bay or Amazon could not exist without public-key cryptography. Since 30 years the theory of cryptography has developed considerably. However, cryptography is not only a theoretical science; namely at some point the cryptographic algorithms must be implemented on physical devices, like PCs, smart-cards or RFIDs. Then problems arise: in general smart-cards and RFIDs have limited computing power and leak information through power consumption and electro-magnetic radiations. A cryptographic algorithm which is perfectly secure in theory can be completely insecure in practice if improperly implemented. Therefore, the aim of this proposal is to take into account every aspect of the implementation of secure systems in the real world, from the mathematical algorithms to the cryptographic protocols, and from the cryptographic protocols to their implementation in the real world. This allows creating a bridge between theoretical research in cryptography on the one side and its applications and the end users of the new technology on the other side. When dealing with cryptographic protocols, we will work in the framework of provable security: every security goal will be clearly defined, and every new cryptographic scheme or protocol should have a proof that the corresponding security goal is achieved, based on some well defined computational hardness assumption. When dealing with cryptographic implementations, we will try to cover all known side-channel attacks: timing attacks, power attacks, cache attack, etc.

Results:

Due to administrative reasons the actual start of the project is postponed to the first half of 2011.

Secure, Reliable and Trustworthy Voting Systems	
Acronym	SeRTVS
Reference	I2R-DIR-PFN-09IS06
Head of Project	Prof. Dr. Peter Ryan
Funding	FNR-Core, 333000€ FNR-AFR, 216216€ IMT Luca, 130000€ University of Melbourne, 60000€ UL, 268596€
Running Time	01/02/2010 - 01/02/2013

Members:

Peter Ryan

Domain(s):

Electronic voting

Partner(s):

- University of Surrey, U.K.
- University of Birmingham (U.K.)
- IMT Institute for Advanced Studies Lucca, Italy
- University of Melbourne, Australia

Description:

Ensuring that the outcome of an election is demonstrably correct while maintaining ballot privacy and minimising the dependence on election officials has been a challenge since the dawn of democracy. For over a century the US has experimented with various technologies to try to make voting easier and more secure. All of these have proved problematic, most notably the more recent use of touch screen machines. The danger here is that the outcome is critically dependent on the correct execution of the code running on the voting devices.

Recent research has explored the use of modern cryptography to address this challenge. Significant advances have been made, in particular advancing the notion of “voter-verifiability”: allowing voters to confirm that their vote is accurately counted while avoiding threats of vote buying or coercion. Notable amongst such schemes is the Prêt à Voter system, proposed by the PI in 2004 and subsequently developed to make it more usable, secure

and flexible. The Prêt à Voter approach is widely regarded as one of the most secure and useable of such schemes and is arguably the most promising in terms of providing a practical scheme for real-world use.

Despite the successes achieved in this field, the issues of robustness and trustworthiness remain open. Verification procedures are a part of most proposed systems, intended to offer trust. However, systems universally lack procedures in case the verification finds errors and the complexity of the verification procedures often undermines trust instead of bolstering it.

The aim of the SeRTVS project is to develop and evaluate designs for practical, secure and trustworthy voting systems. Such schemes should yield a demonstrably correct outcome of the election while guaranteeing ballot privacy. Furthermore, such systems must be sufficiently simple to use and understandable as to gain widespread acceptance by voters and other stakeholders. The starting point will be the existing Prêt à Voter and Pretty Good Democracy schemes. Vulnerability or deficiencies identified during the evaluation will be addressed by enhancements to the scheme.

To date, very little has been done to investigate robust recovery mechanisms for voting systems. The project will develop effective recovery mechanisms and strategies. The project will also investigate the issues of public perception and trust of verifiable systems. It is not enough for the system to be trustworthy; it must also be universally perceived as trustworthy. A goal therefore is to measure and advance public understanding and trust in such schemes.

Results:

In the course of the project, Dr. Gabriele Lenzini was recruited as a post-doctoral researcher to start in February 2011. The project staged the International Summer School on Secure Voting (**SECVOTE 2010**) in Bertinoro (Italy) jointly with the TVS project. Research results were published in the proceedings of ESORICS 2010 [106] and INDOCRYPT 2010 [103].

Model-Driven Validation and Verification of Resilient Software Systems	
Acronym	MOVE RE
Reference	F1R-CSC-PFN-09IS02
Head of Project	Prof. Nicolas Guelfi
Funding	FNR-CORE, 265 000€
Running Time	1/5/2010 – 30/4/2013

Members:

Levi Lucio, Yasir Khan, Qin Zhang

Domain(s):

Software Engineering, Security, Dependability, Resilience, Model Checking, Model Driven Engineering

Partner(s):

- University of Luxembourg, Luxembourg
- University of Geneva, Switzerland

Description:

Verification and Validation of software have nowadays clear meanings in the context of Model- Driven Development. With test based verification we worry about producing a set of test cases that will, on the one hand find faults in an implementation - also called in the test literature System Under Test (SUT) - and on the other hand increase trust in the final product. With validation we worry about understanding if the model we are using as reference for implementation and for extracting test cases from is sound. Formal validation is often achieved by mechanically proving properties the model should satisfy. For example, dynamic properties could be expressed in a temporal logic and static properties on the system state could be expressed using logical invariants and then verified on the system's model. In this project we will focus our attention on the application of validation and verification techniques to the Model Driven Engineering of systems where resilience mechanisms are explicitly modelled and implemented according to that model. Resilience corresponds to the fact that a system has the capability to adapt to harmful events and recover to a stable state or at least continue operation in a degraded mode without failing completely. These harmful events might cause the fundamental security properties (confidentiality, integrity and availability) to be violated. With this project we aim at improving the state of the art of the construction of reliable resilient systems by using verification and validation techniques within the context of Model Driven Development (MDD). The current trend of Software Engineering is to increasingly reason about the system being built at the model level by using appropriate Domain Specific Languages (DSL) for each conceptual domain. In this project we will concentrate on resilience and materialize it as a DSL. Model composition techniques can then be used in order to compose resilience features expressed in the resilience DSL with other domains equally defined as DSLs. When the composed model is validated, verification techniques can then be used to insure the resilience properties are well implemented. We will tackle this problem both at a theoretical and a practical level.

Results:

Since the beginning of the project in May 2010 we have had two main results. The first one is an abstract definition of resilience from a software engineering perspective. This work is accessible as a technical report in [249]. It has also been submitted to the journal "Transactions on Software Engineering and Methodology" and for which approval is pending. The second result is an operational definition of resilience using a model driven approach and model checking tools. The work is based on [249] and is accessible also as a technical report in [251]. A paper based on this technical report has been submitted to TOOLS 2011. Both these papers concern work packages 1 and 2 of project MOVERE.

Two PhD. students, Yasir Khan and Qin Zhang have been hired for working for MOVERE funded by the FNR AFR program. Qin Zhang has started at the University of Geneva in November 2010 and is currently familiarizing himself with the project and the tools he will be using. Yasir Khan has filed a visa demand at the Belgium embassy in his home country and is expected at the Luxembourg in a few months.

Managing Regulatory Compliance: a Business-Centred Approach	
Acronym	MaRCo
Reference	I2R-DIR-PFN-09IS01
Head of Project	Prof. Dr. Pierre Kelsen
Funding	FNR-CORE, 749K €
Running Time	01/05/2010 – 30/04/2013

Members:

Pierre Kelsen, Leon van der Torre (both University of Luxembourg)

Domain(s):

compliance, business process modeling, normative requirements

Partner(s):

- NICTA Queensland Research Laboratory, Australia
- University of Osnabrueck, Germany

Description:

The processes that underpin the businesses of our everyday lives are governed by regulations of ever growing complexity. In this context, it is important (a) to be able to describe these complex regulations rigorously, precisely and

unambiguously, (b) that business practitioners are actually able to specify both regulations and business processes, and (c) to be able to check in an automated way that business processes comply with their underlying regulations. This project proposes to tackle these three issues. On one hand we want to improve existing approaches to formally describe (or model) norms. On the other hand we would like to make this practical and usable by practitioners in such a way that the mathematical based formalisms involved in norm specification do not constitute a barrier to practitioners that know the business domain, but not the underlying mathematical formalism being used and so we propose a visual-based approach to norm specification. Finally, we intend to check the compliance of business processes against the norms that govern them in order to be able to detect in an automated way business processes that violate their underlying regulations.

The proposed research project aims at creating added value for service-related industries (e.g. in the banking sector) by making the specification of business processes and norms rigorous and precise yet accessible to domain experts, and enabling an automated approach to compliance checking. This should provide means to ensure that services are aligned with their underlying local and international regulations. With the growing need for regulatory compliance this will strengthen the expertise in service science in Luxembourg.

Security TEsting for Resilient systems	
Acronym	SETER
Reference	F1R-CSC-PFN-08IS01
Head of Project	Prof. Nicolas Guelfi
Funding	FNR-CORE, 438,300.00 €
Running Time	01/05/2009 – 30/04/2012

Members:

Nicolas Guelfi, Yves Le Trahon, Ayda Saidane, Iram Rubab

Domain(s):

Security, Resilience, Model based Testing, Requirement engineering, Software architecture, AADL

Partner(s):

- University of Luxembourg
- Telecom Bretagne, France

Description:

Resilient systems can be viewed as open distributed systems that have capabilities to dynamically adapt, in a predictable way, to unexpected and harmful events, including faults and errors. Engineering such systems is a challenging issue which implies reasoning explicitly and in a consistent way about functional and non-functional characteristics of systems. The difficulty to build resilient systems and the economic pressure to produce high quality software with constraints on costs, quality, security, reliability, etc. enforce the use of practical solutions founded on scientific knowledge. One of these solutions is to propose an innovative testing process. Testing is an activity that aims at both demonstrating discrepancies between a systems actual and intended behaviours and increasing the confidence that there is no such discrepancy. One of the main features of a system to test is the security of the system, especially for those which are safety or business critical. The security of a system classically relates to the confidentiality and integrity of data as well as the availability of systems and the non-repudiation of transactions. Testing security properties is a real challenge, especially for resilient systems which have the capability to dynamically evolve to improve the security attributes. The aim of the SETER project is to define a new testing approach that will ease the verification of resilient programs that implement this security property. This approach must be aware that confidentiality and integrity can be compromised in many different ways (and consequently the resilient system can evolve in many different ways too), that availability and non-repudiation guarantees are difficult to ensure, and that it must be compliant with the other tests addressing the core functionalities of the system. Current trends advocate the idea that resilience should become an integral part of all steps of software development. Moreover, testing is important for detecting errors early in the development life cycle. The earlier an error is detected, the easier and cheaper it is to resolve. Therefore, the objective of the SETER project fits with these ideas by proposing new security testing approaches for resilient systems the earlier possible during the software development lifecycle to propose more secure and more reliable system.

Results:

- result 1 A Formal Framework for Dependability and Resilience (WP 3 - Resilient System Specification and Security Requirements)
- result 2 model based security testing approach (WP 4 - Test Case Specification and Selection)
- result 3 AADL adaptation for expressing resilience requirements (WP 3 - Resilient System Specification and Security Requirements)

Trust-assurance for critical infrastructures in multi-agents environments	
Acronym	TITAN
Reference	F1R-CSC-PFN-08IS21
Head of Project	Dr. Benjamin Gateau
Funding	FNR-CORE, 108000€
Running Time	1/01/2009 – 31/12/2010

Members:

Pascal Bouvry, Grégoire Danoy, Marcin Sereczynski, Thomas Schaberreiter.

Domain(s):

Trust, Security, Critical Infrastructures, Metrics, Policy Engineering, Governance, Responsibility, Distributed and Multi-agents Systems, Aggregation techniques, Constraints in Policies, Organisational Models.

Partner(s):

- North Dakota University, USA
- VTT Technical Research Centre of Finland
- Ecole Nationale Supérieure des Mines de St-Etienne, France

Description:

The University of Luxembourg work-packages aim at providing innovative methodologies to efficiently and effectively retrieve and manage trust metrics, such as access rights, trust measures, and reputation in critical infrastructures.

Results:

Major achievements of the WP5 are listed in the following:

- Model for Trust Management to avoid Collusion in Mobile Ad Hoc Networks [180].
- It was demonstrated that in specific networking conditions (where a certain number of nodes have utilitarian preferences) a selfish free-riding approach (denoted as ALLD) outperforms TFT-based strategies. It minimises node's battery usage at the expense of other nodes that use the ALLC strategy (unconditionally cooperative strategy representing utilitarian preferences) [182].
- The Cost of Altruistic Punishment in Indirect Reciprocity-based Co-

operation in Mobile Ad Hoc Networks [181].

- The necessary cooperation between wireless mobile ad hoc network users on packet forwarding can be reached by means of a distributed cooperation enforcement mechanism, in which a significant role is played by a trust system. Such a system enables nodes to evaluate the trustworthiness of other network participants before getting involved into mutual forwarding interactions with them. Two mechanisms underlying cooperation in ad hoc networks have been analyzed: direct and in- direct reciprocity. On the basis of these mechanisms a new classification of trust data as personal and general has been introduced [183].

EnerGy-efficient REsourceE AllocationN in AutonomIc Cloud CompuTing	
Acronym	GreenIT
Reference	F1R-CSC-PFN-08IS21
Head of Project	Prof. Dr. Pascal Bouvry
Funding	FNR-CORE, 432000€
Running Time	1/01/2010 – 31/12/2012

Members:

Pascal Bouvry, Samee U. Khan, Thomas Engel, Zdislaw Zuchanecki, Johnatan Pecero, Beranbe Dorronsoro, Marcin Seredynski, Grégoire Danoy, Sébastien Varrette, Alexandru-Adrian Tantar, Dzmitry Kliazovich, Radha Thanga Raj, Frédéric Pinel, Cesar Diaz.

Domain(s):

Energy-efficiency, resource management, heterogeneous computing, multi-objective optimization, multi-agent systems, parallel and distributed computing, telecommunication networks, cloud computing.

Partner(s):

- North Dakota University, USA
- LuxConnect

Description:

The project GreenIT aims to provide a holistic autonomic energy-efficient solution to manage, provision, and administer the various resources of Cloud-Computing (CC) data/HPC centers.

The main research challenges that will be tackled to achieve the holistic approach are:

- Development of a multi-objective mathematical meta-model: CC is a complex system of numerous pervasive devices that request services over heterogeneous network infrastructures from a data center that is energy gobbler. Because each computing entity's performance is defined uniquely, we must develop a multi-objective meta-model that can adequately define a unified and performance metric of the whole system. The multiple constraints and objectives dealing with the quality of service (QoS), cost and environment impact must be formulated and their relationship analyzed.
- Develop resource management and optimization methodologies: With several possible objectives and constraints, the meta-models must result in multi-objective multi-constraint optimization problems (MOP). Green-ICT will develop, refine, and evolve solutions for MOP that will primarily be based on metaheuristics (e.g. multi-objective evolutionary algorithms, multi-objective local search, hybrid metaheuristics).
- Develop autonomic resource management: The anytime anywhere slogan only will be effective when an autonomic management of resources can be achieved. The resource allocation methodologies developed must go further refinement such that the system at hand is self-healing, repairing, and optimizing. In particular, it is our intention to utilize multi-agent systems (MAS) that can learn to adapt (machine learning methodologies) and gracefully evolve to adapt (evolutionary game theoretical methodologies).

Results:

For the computational aspects (WP1), the studied models include the modern architectures based on multi-core chips and also GPU (Graphical Processing Units). Different new approaches mixing load-balancing methods coupled with DVS (Dynamic Voltage Scaling) and power-down features have been proposed, including a multi-objective approach. Several of the newly proposed algorithms outperformed state-of-the-art for the proposed case study [206], [200], [209], [216].

At the level of memory-aspects (WP2), after surveying existing models covering the notion of elementary storage modules (SDRAM) and Non-Uniform Memory Architectures (NUMA) architectures, we proposed a new model able also to take into account memory contention for multi-core CPUs. Based on a sensibility analysis we established the list of relevant parameters and built a model that helps measuring the memory contention issues

on multi-core chips. Experimental validation of this model is foreseen in WP4/WP5.

For the communication aspects (WP3), distributed cloud-based data centers have been modeled, including the multi-layer interconnect. A network simulator (GreenCloud) has been designed and implemented as an open source project. The proposed network oriented model has been implemented on GreenCloud and used to validate different load balancing policies from web server to computing intensive activities.

Several work of editorship and organization of new events have been also undertaken that will ensure additional impact in the following years (including editorship of a special issue of the Journal of Supercomputing, published by Springer).

Two websites have been created to contain the project information: <http://greenit.gforge.uni.lu> and <https://gforge.uni.lu/projects/greencloud/> to provide access to the energy efficiency simulator for distributed data centers developed in the framework of the GreenIT project.

Security Games	
Acronym	S-GAMES
Reference	C08/IS/03
Head of Project	Prof. Dr. Leon van der Torre
Funding	FNR-CORE, 314000€
Running Time	01/04/2009-31/03/2012

Members:

Leon van der Torre, Sjouke Mauw, Wojciech Jamroga, Matthijs Melissen

Domain(s):

- Game theory
- Security protocols
- Non-zero sum games
- Imperfect information games
- Attack–defense analysis

Partner(s):

- GAMES Network

Description:

Information security is not a static black-and-white system feature. Rather, it is a dynamic balance between a service provider trying to keep his system secure and an adversary trying to penetrate or abuse the service. Such interplay can be considered as a game between the adversary and the service provider and the field of game theory provides methods and tools to analyse such interactions.

Games for verification and design have been studied in computer science for the last ten years. This fundamental research into extending and complementing traditional verification approaches from formal methods with game theoretic reasoning is paving the way for more effective verification tools. These developments are of particular interest to the field of security, in which formal verification has always played an important role. The purpose of the project is to study how these new developments can be used to strengthen current analysis and verification techniques in information security.

The project has two main lines of research: 1) A study of the use of game-theoretic methods in the field of security, resulting in requirements on game-theoretic methods for security. 2) The development of novel verification methods based on the combined use of formal verification techniques and a game theoretic approach, and its application to the field of security.

For the first line, two areas in security are selected for which the application of these techniques seems particularly promising: fair exchange protocols and attack–defense analysis. The second line focuses on the interplay of finite and infinite games, mathematical logic and automata theory, in particular on analysis techniques for infinite-state systems, linear-time model checking, and game models for protocols.

The S–GAMES project is a joint project of the SaToSS group and the ICR group of Prof. Dr. Leon van der Torre.

Results:

The research is conducted in several directions in parallel. Apart from a detailed study of the existing literature on game models, reasoning about games, and verification of properties of multi-agent systems, we have already opened up some promising research paths:

- We studied the complexity of model checking problems for several game logics, and detected important errors in the existing literature on the subject. The most important part of the work was published in a conference paper at AAMAS 2010 [174]; an extended journal

version in AI Communications followed [43]. A comprehensive survey of existing and new results in the field was published in [175].

- We proposed a preliminary framework for verification of strategic properties of multi-agent programs [173].
- We studied the relationship between game models coming from cooperative and noncooperative game theory, showing that an existing well-known result is incorrect, and giving the correct characterization [172]. In a related study, we began a systematic exploration of different semantic variants of strategic logics [171].
- We continued studies on combining strategic logics and description logics. A journal publication in *Electronic Notes in Theoretical Computer Science* followed in [65].
- Together with members of the CORE project ATREES, we studied the relation between game-theory and attack–defense trees [179].

In addition to joint activities with our sister project ATREES, we have started collaboration with several internationally recognized experts. These include joint work with Jean-Francois Raskin from the Free University of Brussels on games for verification, Wojciech Penczek from the IPI PAN Warsaw on verification of distributed systems and security properties, Jürgen Dix from Clausthal University of Technology on reasoning about games and game-like scenarios, Valentin Goranko from the Technical University of Denmark Copenhagen on verification of temporal and strategic properties of systems, and Hans van Ditmarsch from the University of Sevilla on unconditional security and analysis of epistemic games. The collaboration is facilitated by mutual visits, research discussions, and developing ideas for future publications.

Finally, members of S–GAMES were co-organizing and co-chairing two international workshops on logics in multi-agent systems, namely LAMAS 2010 (3rd Workshop on Logical Aspects of Multi-Agent Systems) and CLIMA XI (Computational Logic in Multi-Agent Systems). They also served as co-editors of the proceedings [260, 261].

The Dynamics of Argumentation	
Acronym	DYNARG
Reference	F1R-CSC-PFN-09DYNAR
Head of Project	Prof. Dr. Leon van der Torre
Funding	FNR-INTER/CNRS
Running Time	01/10/2009 – 31/09/2012

Members:

Richard Booth, Tjitze Rienstra, Martin Caminada, Emil Weydert

Domain(s):

Argumentation theory, Belief dynamics, Multi-agent systems

Partner(s):

Université d'Artois, Lens, France (Dr Souhila Kaci)

Description:

Artificial Intelligence is a science that aims to implement human intelligence. For this purpose it studies the behaviour of rational agents. Pertinent information may however be insufficient, or there may be too much relevant but partially incoherent information. Different theories have been proposed for decision-making in these contexts. In particular, the growing development of multi-agent systems requires the handling of collective decisions and of information coming from different sources. Moreover, in multi-agent systems agents need to interact in order to inform, convince, and negotiate with other agents. Argumentation theory is a suitable theory to support such interactions. In this project we will create an abstract theory of dynamic argumentation in which arguments/conflict relations can be added/removed. We will also investigate the aggregation of argumentation frameworks to model the interaction among arguing agents. To this end we will, e.g., develop new notions of distance between argument graph labelings in order to define when an agent's position can be said to be "close to" or "far" from that of another. Finally we plan to apply the dynamic argumentation theory to dialogue between agents. We want to study these problems both from within *abstract* argumentation frameworks, in which the focus is on how arguments interact with each other without specifying the actual form of the arguments, as well as using more *concrete* representations of what an argument consists of (e.g., a number of explicit, possibly defeasible "rules" supporting a "conclusion").

Results:

- Literature survey completed.
- Preliminary investigations carried out into the notion of distance between different possible labelings of an argumentation graph.
- Development of a procedure for iterated revision with collections of instantiated arguments in the form of defeasible conditional evidence [138].
- The study of operations of *contraction* (i.e., operations in which a rule-

base is modified in order to avoid supporting unwanted conclusions) in Horn Logic, a simple rule-based formalism which can be used to construct arguments [137, 135].

- Since 1/11/2010, Tjitze Rienstra is working as a PhD student within the topic of DYNARG.

4.1.3 UL Projects

A Formal Approach to Enforced Privacy in e-Services	
Acronym	EPRIV
Reference	PUL-09EPRI
Head of Project	Prof. Dr. Sjouke Mauw
Funding	UL, 254955€
Running Time	01/05/2009–30/04/2012

Members:

Sjouke Mauw, Jun Pang, Hugo Jonker, Naipeng Dong

Domain(s):

enforced privacy, verification, formal modelling, e-services

Partner(s):

- ENS Cachan, Paris, France

Description:

Privacy has been a fundamental property for distributed systems which provide e-services to users. In these systems, users become more and more concerned about their anonymity and how their personal information has been used. For example, in voting systems a voter wants to keep her vote secret. Recently, strong privacy properties in voting such as receipt-freeness and coercion-resistance were proposed and have received considerable attention. These notions seek to prevent vote buying (where a voter chooses to renounce her vote). These strong notions of privacy, which we will call enforced privacy, actually capture the essential idea that privacy must be enforced by a system upon its users, instead of users desiring privacy.

The first aim of this project is to extend enforced privacy from voting to other domains, such as online auctions, anonymous communications, healthcare, and digital rights management, where enforced privacy is a paramount requirement. For example, in healthcare, a patient's health record is private information. However, a patient contracting a serious disease is at risk of

discrimination by parties aware of her illness. The inability to unveil (specific parts of) the health record of a patient is a minimal requirement for her privacy.

The second aim of the project is to develop a domain-independent formal framework in which enforced privacy properties in different domains can be captured in a natural, uniform and precise way. Typically, enforced privacy properties will be formalized as equivalence relations on traces, which take into account both the knowledge of the intruder and the users. Within the framework, algorithms can be designed to support analysis of e-service systems which claim to have enforced privacy properties. In the end, the formalization and techniques will be applied to verify existing real-life systems and to help the design of new systems with enforced privacy properties.

Results:

- We studied the interaction between privacy and verifiability in voting. Our results classify both voting and privacy as instances of linkability between entities, which we can formalise in a trace-based setting. This work was published at ICICS'10 [167].
- We participated in a joint research effort resulting in a version of the *Prêt à Voter* voting system, which is versatile in the sense that one input form caters to various ways of aggregating the votes. This result was published at Indocrypt'10 [103].
- We updated earlier work examining privacy in voting. We incorporated an approach based on attack trees, and added an initial categorisation reasoning from an intruder's point of view, on top of a formalisation of enforced privacy in epistemic logic. This result was published in a Springer-Verlag LNCS compilation work [166].
- We formalised the notion of enforced privacy for online auctions. Our formalisation followed an existing framework for privacy in voting by Delaune, Kremer and Ryan. We automated the verification (in the applied pi calculus), and applied the result to one auction protocol, confirming its claim of enforced privacy for non-winners. This result was published at FAST'10 [161].
- We co-organised the SecVote summer school in Bertinoro, Italy. There were 40 attendees from 15 different countries, taught by 12 lecturers of international repute.

Embedded Systems Security	
Acronym	ESS
Reference	F1R-CSC-PUL-08ESSE
Head of Project	Prof. Dr. Alex Biryukov, Prof. Dr. Jean-Sebastien Coron, Prof. Dr. Sjouke Mauw
Funding	UL, 499514€
Running Time	01/10/2008 - 31/01/2012

Members:

Alex Biryukov, Jean-Sebastien Coron, Sjouke Mauw, Ralf-Philipp Weimann, Chenyi Zhang

Domain(s):

Verification, Security Protocol, Model Checking

Description:

The goal of this project is to study cryptosystems and secure protocols for embedded systems (mobile phones, PDAs, smartcards, RFID tags). This is currently an important area of research due to proliferation of portable information processing devices and their penetration in our everyday life. This process is driven by public demand and by the industry. By working together with the industry, the academic research can provide necessary tools in order to procure information security and privacy which becomes more and more important (and often is lacking) in the digital world. The project currently is structured as follows: cryptography for embedded systems (secret key and public key), secure protocols for embedded systems, implementation aspects, biometrics and privacy issues, wireless security. This is a joint project of the SaToSS group with LACS professors Alex Biryukov and Jean-Sebastien Coron.

Results:

Achievements of the SaToSS group:

- Design and analysis of security protocol by model checking (2 coauthored paper produced)
- Verification of secrecy and confidentiality properties (1 coauthored paper produced)
- Study of game semantics for verification (work in progress)

Achievements in the LACS group:

- Analysis and Improvement of the Random Delay Countermeasure of CHES 2009 [213].
- Fault Attacks Against EMV Signatures (CT-RSA 2010).
- Fault Attacks and Countermeasures on Vigilant's RSA-CRT Algorithm (FDTC 2010).
- SPAKE: A Single-Party Public-Key Authenticated Key Exchange Protocol for Contact-Less Applications (FC 2010).
- Reverse-engineering of the DECT standard cipher from hardware (FSE 2010).

Furthermore, we worked together (in the context of the deDECTed.org project) with the DECT Forum and the ETSI SAGE group to remedy the security problems we found in future versions of the DECT standard.

Security and Cryptography in the Real World	
Acronym	SECRYPT
Reference	F1R-CSC-PUL-07SECR
Head of Project	Prof. Dr. Jean-Sébastien Coron
Funding	UL, 950000 €
Running Time	01/01/2007 - 31/08/2010

Members:

Jean-Sébastien Coron, Alex Biryukov, Volker Müller, David Galindo, Ilya Kizhvatov, Avradip Mandal, Jean-François Gallais, Bin Zhang

Domain(s):

Cryptography, Information Security, Security Proofs

Description:

Today, information technology has expanded to encompass most facets of our daily lives - at work, at school, at home for leisure or learning, and on the move - and it is reaching ever-widening segments of our society. The Internet, e-mails, mobile phones, etc. are already standard channels for the information society to communicate, gain access to new multimedia services, do business or learn new skills. The recent "digital revolution" and widespread access to telecommunication networks have enabled the emergence of e-commerce, which will most likely deeply alter the very concept of business in the near future. This proliferation of digital communications has raised new concerns in terms of security: for example, copyright protection,

access rights management and privacy protection. Security is an interdisciplinary subject, drawing from several fields: cryptography, network security, algorithmic number theory, software and hardware engineering, formal verification, AI, signal processing, legal issues, data and text mining, anomaly and fraud detection, any many more. In this context, we find it very appropriate to outline in this document a "Security and Cryptography in the Real World" research program proposal. This research program builds on an existing expertise in the relevant fields among the University's faculty members, and its goal is to bring together specialists of the different fields mentioned above to address the problems of security in a global and really efficient way. This research program would therefore prove to be a very innovative and profitable step towards the advancement of the state of the art in a field that is sure to be of paramount importance in tomorrow's society.

Results:

The achievements of the LACS group in the course of this project include the following:

- New attacks on the PKCS#1 v1.5 encryption standard (published in the proceedings of ACNS 2010).
- Secure delegation of elliptic-curve pairing computations (published in the proceedings of CARDIS 2010).
- Efficient indifferentiable hashing into ordinary elliptic curves (published in the proceedings of CRYPTO 2010).
- A domain extender for the ideal cipher (published in the proceedings of TCC 2010).
- Multiset collision attacks on reduced-round SNOW 3G and SNOW 3G[⊕] (published in the proceedings of ACNS 2010 [107]).
- Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds (published in the proceedings of EUROCRYPT 2010).
- Analysis of the SNOW 3G[⊕] resynchronization mechanism (proceedings of SECURE 2010 [178]).

Adaptive High-gain Extended Kalman Filter and Applications	
Acronym	AHEKFA
Reference	N/A
Head of Project	Prof. Dr. ing. Juergen Sachau
Funding	Junior Researcher contract, University of Luxembourg project: RAIP.
Running Time	2006 - 2010

Members: Nicolas Boizot

Domain(s): Process control, Observers for nonlinear Systems, Applied mathematics, High-gain Extended Kalman Filter

Partner(s): University of Burgundy (Prof. Eric Busvelle, co-directeur de thèse)

Description: The work concerns the “observability problems e.g. the reconstruction of a dynamic process’s full state from a partially measured states for nonlinear dynamic systems. The Extended Kalman Filter (EKF) is a widely-used observer for such nonlinear systems. However it suffers from a lack of theoretical justifications and displays poor performance when the estimated state is far from the real state, e.g. due to large perturbations, a poor initial state estimate, etc.

We propose a solution to these problems, the Adaptive High-Gain (EKF).

Observability theory reveals the existence of special representations characterizing nonlinear systems having the observability property. Such representations are called observability normal forms. A variant of the EKF based on the usage of a single scalar parameter, combined with an observability normal form, leads to an observer, the High-Gain EKF, with improved performance when the estimated state is far from the actual state. Its convergence for any initial estimated state is proven. Unfortunately, and contrary to the EKF, this latter observer is very sensitive to measurement noise.

Our observer combines the behaviors of the EKF and of the high-gain EKF. Our aim is to take advantage of both efficiency with respect to noise smoothing and reactivity to large estimation errors. In order to achieve this, the observer automatically switches between two modes, based on a parameter value that is the heart of the high-gain technique. *Voilà*, the Adaptive High-Gain EKF.

A measure of the quality of the estimation is needed in order to drive the adaptation. We propose such an index and prove the relevance of its usage. We provide a proof of convergence for the resulting observer, and the final algorithm is demonstrated via both simulations and a real-time implementation. Finally, extensions to multiple output and to continuous-discrete systems are given.

Results:

- The initial algorithm developed during the Ph.D. -for single output systems in the continuous time framework- has been extended to the

multiple output case, and to the continuous discrete framework [17].

- A detailed proof of the existence of upper and lower bounds for the matrix solution to the Riccati equation (of the extended Kalman filter) has been done for the continuous discrete setting. Although this result is used in some publications, such a detailed proof didn't appear in the literature so far.
- An article that details the proof has been written, submitted to Automatica and accepted for publication in 2010.
- The Ph.D. has been defended by Mr. Boizot (mention: Outstanding).

Better e-Learning Assignments System Technology	
Acronym	BLAST
Reference	F1R-CSC-PUL-10BLAS
Head of Project	Prof. Dr. Denis Zampuniéris
Funding	UL, 165000€
Running Time	01/09/2010 - 31/08/2012

Members:

Sergio Dias, Shahed Parnian, Denis Zampuniéris

Domain(s):

Proactive computing, E-learning, Online assignments management system

Description:

The project aims at the design and implementation of a proactive online assignments system for blended teachings at the University of Luxembourg, which will actively support students as well as teachers in a collaborative way.

The main output product of this research and development project will be an online assignments system with advanced features while remaining easily usable by every user beginner or expert, that is useful for our teachings and which will be based on software currently in use at the UL.

The design will rely on the innovative concept of proactive computing applied to the e-learning technologies field. Indeed, instead of waiting for user interaction like in existing reactive learning management systems, our proactive assignments system (embedded into a standard e-learning platform) will allow us to define analysis and management rules that will be applied autonomously by the system to support and drive the workflow, when a teacher online assigned tasks to students.

The possible rules will range from simple reminders and notifications to both parties, to the most elaborated automatic detection of potential problems based on successive detection of (non-) events over a period of time.

Model-Driven Engineering using a Declarative Behavioural Description Language	
Acronym	MEDAL
Reference	F1R-CSC-PUL-08MEDA
Head of Project	Prof. Dr. Pierre Kelsen
Funding	UL, 171K€
Running Time	01/10/2008 – 30/09/2011

Members:

Pierre Kelsen, Nuno Amalio, Christian Glodt

Domain(s):

model-driven software development, executable modeling, complexity

Description:

In model-driven software development models are the primary artifacts for constructing software. Model composition or the process of composing simpler models into more complex models helps in mastering the complexity of model-driven development. Most of the current model composition techniques can be viewed naturally as model transformations taking two input models and producing one output model. In our work we have introduced a new composition technique for building executable models. It has several properties that traditional composition techniques do not have: it is additive rather than transformational; it can be applied to any meta-model; and it has a formal semantics.

The present project will investigate the power of our composition technique with respect to existing composition techniques. In particular we will compare our technique with approaches from aspect-oriented modeling that are typically used to express crosscutting concerns. The project will investigate whether our approach can be extended to match the power of these techniques; and/or how it can complement the existing approaches in modeling systems in a more straightforward, elegant, and light-weight manner. The main goal is to enhance our current modeling framework and tool for executable modeling with new model composition techniques so that they can handle not only the academic examples studied so far but can be used effectively on larger systems.

Results:

- 3 publications in peer-reviewed conferences and one journal publication

Resource Allocation in Delay and Disruption Tolerant Networks	
Acronym	RAID
Reference	N/A
Head of Project	Prof. Dr. Simin Najdm-Tehrani
Funding	UL
Running Time	01/09/2007 - 01/09/2011

Members:

Simin Najdm-Tehrani Gabriel Sandulescu

Domain(s):

Opportunistic networks, Delay and Disruption Tolerant Networks, Quality of service, Mobile Communications

Partner(s):

- Linköping University, Sweden

Description:

This PhD research project aims to propose new architectures, algorithms and communication protocols in intermittently-connected ad hoc networks, also referred to as delay-tolerant networks (DTNs). One potential interest is to minimize the impact of connectivity interruption when commuting or traveling while controlling the usage of the network resources. Proposed solutions must be founded on sound theoretical background and must be usable by network engineers. When pure analytical framework is not sufficient, a simulation environment or a practical implementation should be used in order to validate research results.

Results:

The results for 2010 have materialised in publications on three related research topics. The first is a collaboration scheme using recent node encounters to estimate resources in the vicinity: energy, buffer space, and bandwidth. Nodes can then autonomously exploit this information in a holistic way, by implementing effective routing strategies, based on the availability of these three resources in node proximity. The results were presented at the Wireless Days 2010 conference. The second is an optimisation framework for store-carry-forward protocols using message replication and message fragmentation with erasure coding. The paper on this topic was published in [226] and was presented at the CTRQ conference. The third is a follow-

up to an earlier research topic, which involves adding fragmentation to our routing protocol (ORWAR). The results were published in a Special Issue on Delay Tolerant Networks, Architecture, and Applications of the Journal of Communications in 2010 [58]

VERIFICATION of fault-tolerant advanced Transactional distributed sYstems	
Acronym	VERITY
Reference	F1R-CSC-PUL-08VERI
Head of Project	Prof. Dr. Nicolas Guelfi
Funding	University of Luxembourg, 364257€
Running Time	01/01/2008 – 31/03/2011

Members:

MSc Federico Wiecko

Domain(s):

Model Driven Engineering, Model Transformation, Dependability, Simulation, Domain Specific Languages

Description:

The VERITY project is a 3 year long research project that aims at developing tool support for (semi) formal languages to allow software engineers to model and verify secure and dependable advanced transactional distributed systems.

Results:

- Creation of the Technical Report (TR-LASSY-10-04) named "An Evaluation of MDE tools in the context of M2M transformations". In that report, an analysis of M2M transformation properties is performed based on previous work done by 'Mens and Van Gorp' and 'Czarnecki and Helsen'. After defining a criteria of comparison, this criteria is later on applied in the comparison of Kermet and ATL model transformation tools.
- **Tools development**
 - Creation of a framework to validate DT4BP (Dependability and Time for Business Processes) models. The goal was to adapt the framework named CAA-DRIP, which was suitable only for manipulating CAA concepts, in order to deal with DT4BP models. Since the semantic domain of CAA does not include concepts

like time constraints, participants, datatypes, etc, several extensions were accomplished on the original framework. In this way, a new framework was created which was called Timed-CAA-DRIP.

- Creation of the tool named TimedCAA2Java. This tool takes as input a Timed-CaaFWrk model and generates Java code customized for the framework Timed-CAA-DRIP. As the result of the execution of this code, a set of traces were obtained. From these traces the analyst, in conjunction with the other stakeholders, can validate the original model in order to detect errors or perform analysis.
- **Case Studies** The case study named "The Patient Diagnosis Running Example", which was originally presented in [59], was specified by using the DT4BP language. The goal for VERITY was to rewrite this example in terms of CAA equivalent concepts and after that, to code it by using specific Java code under the context of framework Timed-CAA-DRIP. After running the example a set of traces were obtained. From these traces, not only the original specification was validated, but it also facilitated the improvement of the framework itself.

Advanced Argumentation Techniques for Trust Management	
Acronym	AASTM
Reference	F1R-CSC-PUL-08AASTM
Head of Project	Prof. Dr. Leon van der Torre
Funding	UL
Running Time	01/05/2008 – 30/04/2012

Members:

Leon van der Torre, Martin Caminada, Yining Wu

Domain(s):

Computational argumentation, Trust

Partner(s):

University of Luxembourg

Description:

The overall aim of AASTM is to enhance today's generation of argumentation formalisms and implementations in order to become suitable for a wider variety of real-life applications, such as reasoning about trust. This requires a unified theory that integrates the various forms of argumentation related

functionality, as well as efficient proof procedures and sound and scalable software components.

Results:

- A Labelling-Based Justification Status of Arguments / Wu, Yining; Caminada, Martin [39]
- Transforming Fuzzy Description Logic ALC_{FL} into Classical Description Logic ALCH / Wu, Yining [117]
- An Implementation of Basic Argumentation Components / Podlaskowski, Mikolaj, Wu, Yining, Caminada, Martin [101]
- On the Profitability of Incompetence / E. Staab; M.W.A. Caminada [232]
- A Logical Account of Lying / Ch. Sakama; M.W.A. Caminada; A. Herzig [145]
- On the Existence of Semi-Stable Extensions / Caminada, Martin; B. Verheij [144]
- On the Justification Status of Arguments / Caminada, Martin; Yining, Wu [143]
- An Algorithm for Stage Semantics / Caminada, Martin [142]
- The Many Faces of Deception / Ch. Sakama; Caminada, Martin [141]
- Preferred Semantics as Socratic Discussion / Caminada, Martin [139]
- Manipulation in group argument evaluation / Caminada, Martin; G. Pigozzi; M. Podlaskowski [102]

In 2010, most progress on the AASTM project was related to the fundamentals of argumentation theory. As for the topic of argumentation and trust, some research that was done in 2010 has recently been accepted for the first publication in 2011.

Individual and Collective Reasoning	
Acronym	ICR
Reference	F1R-CSC-LAB-05ILIA
Head of Project	Prof. Dr. Leon van der Torre
Funding	UL-PHD
Running Time	12/03/2008 – 12/03/2012

Members:

Gabriella Pigozzi, Marija Slavkovic, Leon van der Torre

Domain(s):

Judgment aggregation, Group-decision making, Social choice theory, Normative systems

Partner(s):

University of Luxembourg

Description:

Traditional decision-making is driven by the concept of a rational agent who acts in his own best interest by maximizing the expected utility. Opposite to the rational agent modeled as Homo Economicus, people do not make decisions by generating alternative options and by comparing them on the same set of evaluation dimensions; nor do they generate probability and utility estimates for different courses of action. They search for, what Herbert A. Simon called, satisficing, or “good enough” decisions. We define a satisficing decision as one that is determined by making a yes/no estimate for each element of a given set of decision-relevant criteria. The aim of this project is to investigate how groups of artificial agents can reach satisficing decisions. The contribution of the thesis is threefold. For the area of multi-agent systems we propose a new way in which group decisions can be reached. As a show-case, we apply our decision-reaching method to the problem of determining group intentions. For the field of judgment aggregation, our contribution is a new set of judgment aggregation operators. For the field of belief merging, our contribution is the identification of a new problem of iterated belief merging.

Results:

- In order to avoid an untenable collective outcome, individuals may prefer to declare a less preferred judgment set. Thus, the prospect of an individual trying to manipulate the social outcome by submitting an insincere judgment set is turned from being an undesirable to a “virtuous” (or white) manipulation. In [62] we defined and studied white manipulation as a coordinated action of the whole group.
- In [63] we presented an aggregation procedure providing complete judgment sets, i.e. judgment sets with premises and conclusion. We showed that our procedure satisfies the desirable properties of non-manipulability and it can be modified to preserve unanimity on the premises.
- In order to show the practical applicability of group decision-reaching

through judgment aggregation we studied the problem of determining group intentions based on declared beliefs, or acceptances of the members. In [125] we present a formal model for deciding on collective intentions and study the related group commitment and intention revision problems.

4.1.4 Other miscellaneous projects

Combine Software Product Line and Aspect-Oriented Software Development	
Acronym	SPLIT
Reference	F1R-CSC-PFN-09SPLI
Head of Project	Prof. Dr. Nicolas Guelfi
Funding	UL/FNR, 41 000€
Running Time	01/10/2009 –30/09/2012

Members:

Nicolas Guelfi, Jacques Klein, Jean-Marc Jézéquel, Olivier Barais, Benoit Baudry, Benoit Ries, Vasco Sousa

Domain(s):

Software Engineering, Model Driven Engineering, Software Product Line, Aspect Oriented Modeling, Model Composition, UML

Partner(s):

- CNRS/INRIA, University of Rennes, France
- Public Research Center Gabriel Lippmann

Description:

Software engineering proposes practical solutions, founded on scientific knowledge, to produce and maintain software with constraints on costs, quality and deadlines. The complexity of software increases dramatically with its size. A challenging trade-off for software engineering exists in a reality where the amount of software in existence is on average multiplied by ten every ten years, as against the economic pressure to reduce development time and increase the rate at which modifications are made. To face these problems, many of today's mainstream approaches are built on the concepts of Model-Driven Engineering (MDE), Software Product Line (SPL) or Aspect-Oriented Software Development (AOSD) to foster software reuse. In an emerging MDE context, SPL and AOSD share the common objectives to

reduce the cost and the risk of adapting software systems to wide ranges of new contexts. On the one hand, SPL techniques allow the modeling of product variability and commonalities. A SPL development approach strongly depend on a composition mechanism supporting product derivation from the SPL definition at any level of abstraction (analysis, design, implementation, ...). On the other hand, AOSD proposes new techniques to compose and weave separate concerns which can represent features, but AOSD does not propose mechanism to manage the variability of software. Thus, both approaches complement each other, and the combination of SPL and AOSD paradigms provides an exciting challenge allowing the use of efficient product lines through the whole software development lifecycle. This collaboration aims at investigating further the complementarities between SPL and AOSD approaches in a MDE context. This should make it possible to discover entirely new ways of formally decomposing and recomposing software systems, at a much higher level of abstraction than anything that is available today (notion of modularity based on classes and components). In order to do so, several main technical areas must be addressed:

- Identify the common concepts and the difference between SPL and AOSD to combine the both approaches
- Study the special activity of horizontal model transformation in the context of SPL and AOSD methodologies and to propose a transformation language to support them
- Provide rigorous and generic means to guaranties the consistency between models through aspect weaving and product derivation
- Build a generic AOM weaver with built-in variability mechanism to drive runtime adaptation

The problems inherent to this research project are in the heart of the software engineering problems such as model composition, model transformation, model evolution, model reusability, model consistency, etc.

Results:

- Analysis of tools and proceedings for the development of the generic AOM approach tool, namely analysing and testing the requirements for integration as eclipse plug-in for tool deployment, compatability of this compatibility requirements with the test projects already developed in Kermeta and Drools
- Development and specification of the Aspect metamodel, composed of Pointcut information and Advice, including specification alterna-

tives to be tested during tool development for acersion of the best and clearest specification approach

- Development and specification of a meta-model for internal information exchange within the several steps of the AOM tools execution

Modelling of Business and IT Landscapes addressing Security, Risk and Compliance in a Real-World banking environment (PhD thesis)

Acronym	MBITSRC
Reference	F1R-CSC-PAU-06CRE
Head of Project	Prof. Dr. Thomas Engel
Funding	Credit Suisse and FNR (128.50K€)
Running Time	2005-2010

Domain(s):

IP and software modelling

Partner(s):

- Credit Suisse

Description:

The overall focus is on reusing existing models first, adapting existing models second, and finally create new ones if needed. Further on the focus is on usability and automation of the modelling and checking process. The notion of clickable mathematics came up in this contex.

Results:

- Modeling of secure software
- Composition of large software projects

End-to-end Web Service Security in AspectOriented Programming

Acronym	EWSSAOP
Reference	F1R-CSC-PAU-07LIA
Head of Project	Prof. Dr Thomas Engel
Funding	EPT (75K€)
Running Time	2008 – 2011

Members:

Thomas Engel, Shaonan Wang,

Domain(s):

Network Security

Partner(s):

- EPT

Description:

The monitoring of large network traffic volumes is limited by the existing technological solutions. Monitoring high speed 40 Gbps links is challenged by the already existing work charge on the routing data plane. One of the few activities that can be done is limited to recording and analyzing flow records. IP flow records are simple information records capturing the source, destination, the associated ports, the traffic volume and additional time stamps and flow related status. The natural question is how should these pieces of information be processed. On one side, the number of flow records is huge even for small sized edge routers, and on the other side it's not obvious what information should be analyzed. We have considered this research question in this paper. The main contribution of our paper is twofold: we propose a simple dependency model for IP flow records and show how link based analysis can reveal interesting flow events. We will use in this paper the words IP flow records and NetFlow records interchangeably. We have validated our approach using the proprietary NetFlow data format, but our method is general and can be applied to any flow record format. We aimed in this paper at identifying relevant flow records, where by relevant we understand the records that have generated ulterior network activity. We don't consider that a flow matching a specific signature (application level or based on the involved IP addresses) is relevant per se, but we do consider that flows, having triggered an important follow-up network activity, are relevant. The notion of triggering is linked to a potential dependency relationship among flow records. The best illustration for this is the case of an attacker breaking in over an SSH account. While the SSH related flow traffic is in general not relevant, in this case this could be the case if follow-up activities of the compromised host will be observed: large scale network scanning, rootkit downloading, massive SMTP traffic or botnet membership. For scoring such relevant IP flow records and understanding the most active activities on the network, our approach consists of two major steps. Firstly, with a simple yet efficient dependency model, we discover the causality dependency between NetFlow records. Then, to facilitate analyzing the overwhelming scale of NetFlow dependency graph, we automatically select the most relevant NetFlow records using the link analysis algorithm HIT. To the best of our

knowledge, this is the first attempt to apply HITS algorithm from the web search and bibliometrics domain, in the field of network monitoring.

Results:

We have proposed a data mining approach that leverages pagerank for ranking netflow records that uses a dependency model that captures traffic related information among hosts. We have implemented this approach and published out results in [197, 217, 218]

EPT Vehicular Networks	
Acronym	EPTV
Reference	I2R-DIR-PAU-09EPTV
Head of Project	Prof. Dr. Thomas Engel
Funding	EPT - 2 298 K€
Running Time	01/01/2010-31/12/2014

Members:

Thomas Engel, Raphael Frank, Marcin Seredynski

Domain(s):

Vehicular Ad Hoc Networks

Partner(s):

Entreprise des Postes et Telecommunications Luxembourg - EPT

Description:

A standard for vehicular ad hoc networks is expected during 2011. In 2025, 70% of the vehicle fleet within Europe is predicted to apply to the standards, enabling new services and application. A main goal will be to increase traffic safety and reduce the environmental impact of the vehicular transportation system. The vision of the proposed research project is to develop efficient, secure and reliable communication networks to enable the transformation of the vehicular transport system of today to a greener, smarter and safer system. Recent advances in sensor technology, low power electronics, radio-frequency devices, wireless communications, security and networking have enabled the engineering of intelligent vehicles and intelligent transport infrastructure, which have the potential to drastically increase road safety, decrease cost of transportation and contribute to a sustainable environment. This research will address 3 main areas of vehicular networks: 1) Sensor and Mobile Ad Hoc Networks, 2) Embedded Systems and 3) Applications and Services.

Feasibility Study for Topology Optimization	
Acronym	FSTO
Reference	N/A
Head of Project	Prof. Dr. Thomas Engel
Funding	Ministry of Commerce - 40000 €
Running Time	2010

Members:

Thomas Engel, Jerome Francois, Foued Melakessou

Domain(s):

Network Security

Partner(s):

Ministry of Commerce

Description:

The objective of this project is to propose a network cartography approach for Luxembourg Internet infrastructures as well as a realtime monitoring approach for detecting connectivity issues.

Results:

We have designed and implemented a topology sensor that can be deployed in order to test the reachability and traffic performance of exiting Internet infrastructures. The system runs on embedded Linux devices and is capable to achieve its functionality by advanced selfmanagement paradigms.

Securing Mission Operations using Multi-Level Security	
Acronym	SMO-MLS
Reference	To be defined
Head of Project	Prof. Dr. Thomas Engel
Funding	European Space Agency - 48800€
Running Time	UL - 37077 € 01/11/2010 – 01/11/2013

Members:

Thomas Engel, Daniel Fischer, Knut Eckstein

Domain(s):

Spacecraft mission control systems, MLS security

Partner(s):

ESA/ESOC, Germany

Description:

SMO-MLS is an ongoing research project that aims to providing an enhanced security support at the spacecraft control infrastructure of ESA/ESOC by establishing multi-level security (MLS) solutions on its Mission Control System (MCS). Within this research activity, MLS solutions will ensure an enforced separation of command and control data flows of different sensitivity and classification levels between missions and also between individual payload data flows of the same mission. SCOS-2000 (S2K) is the ESA generic software infrastructure implementing the common features required by a spacecraft MCS. Therefore, a SCOS-2000 MLS prototype is to be developed and built upon an operating system that supports multi-level security (i.e. Security-Enhanced Linux). The primary three objectives of this project and that represent the direct security needs of future space missions are:

- (A) Enforcement of integrity policies between telecommand chain data flows
- (B) Enforcement of integrity policies between telemetry chain data flows
- (C) Confidentiality of third party telecommand chain data flows

This research project will advance the research on the area of MLS systems and will provide an MLS model tailored for spacecraft command and control systems.

Results:

As a result of this project, a prototype MLS system based on current ESA mission control system infrastructure will be developed and implemented. This may include the development of specific protocols and procedures. Such protocols may be subject to standardization.

Self Organizing Security Sensors in highly-distributed IP networks (PhD thesis)	
Acronym	SOSSHIN
Reference	F1R-EDR-LIA-000005
Head of Project	Prof. Dr. Thomas Engel
Funding	SES-ASTRA and FNR - 45K€
Running Time	2007 – 2011

Members:

Thomas Engel, Gerard Wagner

Domain(s):

Adaptative Honeypots

Partner(s):

SES - ASTRA

Description:

The recent research activities have addressed the conceptual design and practical assessment of an adaptive honeypot based on game theory. We have addressed these topics, by proposing a game model for a system level honeypots. The best configuration profile has been determined based on the Nash equilibrium, where the best actions for the honeypot (and for an attacker) have been resulted. This work has been awarded the best paper award at the The 11th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2009) . A lateral research result, regarding the modeling and detection of malicious software has addressed the use of support vector machines and process level intrinsic monitoring. The results have been published [11] as a paper in the proceedings of the Malware 2009 Conference, in Montreal, Canada. We have also addressed a game theoretical model for the Tor anonymisation network, where attacker's and defendant's strategies can be modeled. This work is under current submission. The current work is addressing more complex game models, based on repeated games- this work will identify the pertinent conceptual approaches, the definition of strategies and the identification of the associated equilibriums. The application domain will be twofold: netflow based monitoring (in collaboration with Alexandre Dulanoj) and system/host level monitoring.

Results:

The major outcomes from this project included a new paradigm for adaptive honeypots that leverage game theory and reinforcement learning as underlying conceptual building blocks for smarter honeypots. We have implemented and operated such honeypot and the major publications from this project are one journal publications accepted for 2011 and another one for [20].

Secure Usage and Trust of Mobile Devices in Networks for international banking environments (PhD thesis)	
Acronym	SUTMDNiBE
Reference	F1R-PHY-PUL-06DRE
Head of Project	Prof. Dr. Thomas Engel
Funding	Dresdner Bank and FNR - 45K€
Running Time	2005-2010

Members:

Thomas Engel, Michael Stieghahn

Domain(s):

Access Control

Partner(s):

Dresdner Bank

Description:

Cross-border access to a variety of data such as market information, strategic information, or customer-related information defines the daily business of many global companies, including financial institutions. These companies are obliged by law to keep any data processing legal. Today's solutions for remote access are not able to dynamically adapt their access decisions to the current context. Therefore, they may decide either over-restrictive or under-restrictive, because the basis of a decision is the underlying static access control system.

We focus on the incorporation of legal constraints as a context information into a decision making process for international banking environments. Such constraints account for the identity of the user, who accesses the data, the identity of the customer, whose information is stored as data, and the locations, where the data is hosted and accessed. The locations serve the second purpose to determine which sets of legislation need to be observed [73]. We are implementing our approach in the eXtensible Access Control Markup Language that promotes interoperability between different systems and is widely used as policy definition language [72].

Work of the next period will be the completion and evaluation of the prototype of the law-aware access control. The refinement of the protocol that used for the communication between client and server is also an active task.

Results:

The major outcomes of this project consists in the definition of an access control mechanism for mobile banking applications. We have also proposed a modeling framework for the proposed architecture based on the Common Information Model. The project ended with the successful defense of Michael Stieghahn.

Luxembourgish Early-Warning Analysis and Information Sharing System	
Acronym	LEWIS
Reference	I2R-DIR-PAU-09LEWI
Head of Project	Prof. Dr. Peter Ryan
Funding	Ministry of Economy - 70000€ UL, 29120€
Running Time	01/10/2009 – 31/05/2010

Members:

Richard Clayton (Cambridge)

Domain(s):

Malware, Phishing, Botnets

Partner(s):

Ministry of Economy

Description:

LEWIS is an SnT project funded by the Ministry of Economy to investigate nature and scale of cybercrime in Luxembourg and to investigate ways to counter such crime.

Results:

The project was in a pilot phase in 2010 to investigate the scale of the problem, the state-of-the-art, and to produce a report providing a research agenda with a view to setting up a larger scale project in 2011. This research agenda will be presented to the Ministry of Economy in January 2011. Dr. Richard Clayton of the Security Group in Cambridge has been employed to assist in the LEWIS project.

Developing a Prototype of Location Assurance Service Provider	
Acronym	LASP
Reference	ESA Bidder Code: 52056
Head of Project	Prof. Dr. Sjouke Mauw
Funding	ESA 160000€, SnT 80000€
Running Time	08/12/2010–07/12/2012

Members:

Sjouke Mauw, Jun Pang, Xihui Chen, Gabriele Lenzini

Domain(s):

location assurance, privacy of location assurance, location based services, GNSS network security

Partner(s):

-itrust Luxembourg

Description:

The objective of this project is to develop a prototype to provide a high quality level of assurance in the location information that originates from the GNSS network, while protecting location owners from intrusions into their privacy. We approach these objectives from five perspectives.

Analysis: The objective is to precisely describe the requirements, the execution and threat models, the trust relations and the assumptions on the environment.

Design: The objective is to design an architecture for location information assurance and to develop data protection algorithms and decision logic to find out the appropriate assurance level of the location information. The protocols devoted to security and privacy are also developed and integrated in a service architecture.

Verification: The objective is to analyse the result of decision logic in presence of an attacker and evaluate the quality of the output of the designed algorithms. Moreover, based on existing formal verification approaches, a verification methodology which considers trustworthiness of the service together with user privacy will also be studied.

Validation: The objective is to set up the LAP prototype and perform a set of laboratorial tests in order to assess the overall performance. The robustness and performance is optimized through parameter tuning.

Exploitation: The objective is to define risk management principles and prepare a strategy that should apply to assure the requirements in a largest deployment of the solution.

Results:

The work on the project started on 08/12/2010.

4.2 Grants

4.2.1 AFR

A Formal Approach to Enforced Privacy: Modelling, Analysis and Applications	
Acronym	EPRIV-MAA
Reference	PHD-09-027
Head of Project	Prof. Dr. Sjouke Mauw
Funding	FNR–AFR, 105222€
Running Time	01/12/2009–30/11/2012

Members:

Sjouke Mauw, Jun Pang, Hugo Jonker, Naipeng Dong

Domain(s):

formal methods, verification, model checking, security, privacy, e-services

Partner(s):

ENS Cachan, Paris, France

Description:

The project is part of a peer-reviewed UL research project EPRIV — ‘A Formal Approach to Enforced Privacy in e-Services’. The overall goal of this project is to develop a domain-independent formal framework to express the proposed concept of enforced privacy. We extend the notion of enforced privacy outside the domain of voting. Our formalization will take into account coalition-forming and defensive options. Moreover, within this framework, algorithms to verify these requirements will be developed to facilitate verification with tool support. This generic goal is composed of the following sub-goals:

- Lifting the notion of enforced privacy to other e-service domains such as online auctions, anonymous communications, and healthcare; and formalizing the resulting notions;
- Establishing per-domain formal notions to verify enforced privacy;
- Capturing these notions in a domain-independent formal framework;
- Investigating enhancements to the formal framework to verify privacy.

Results:

- Online auction domain: We finished a domain study in online auction, formalised the notion of enforced privacy in this domain, and did a case study of an online auction protocol (modelled the protocol as well as receipt-freeness and strong secrecy in applied pi, and verified these two properties). Publication: ‘Analysis of a receipt-free auction protocol in the applied pi calculus’ describing our work in online auction has been accepted at FAST’10 [161].
- E-health domain: An extensive study of e-health domain has been performed. Currently we are working on this application domain.

Games for Modelling and Analysis of Security	
Acronym	GMASec
Reference	FNR–AFR PHD-09-082
Head of Project	Prof. Dr. Sjouke Mauw
Funding	FNR–AFR, 105223,44€
Running Time	01/11/2009–31/10/2012

Members:

Sjouke Mauw, Matthijs Melissen, Wojciech Jamroga, Leon van der Torre

Domain(s):

formal methods, game theory, security, imperfect information games, verification, model checking

Partner(s):

- Université Libre de Bruxelles, Belgium
- Colorado State University, USA
- GAMES Network

Description:

Game theory models the strategic interaction among various agents, assuming each of the agents strives to increase his own pay-off. Such an interaction frequently occurs in security problems. Examples are the interaction between the attacker of a system and its defender, or the interaction between two possibly dishonest participants in a security protocol. Therefore game theory is a particularly relevant tool in the field of security.

The GMASec project is executed in the context of the S–GAMES project, and is a joint project of the SaToSS group, headed by Prof. Sjouke Mauw, and the ICR group headed by Prof. Leon van der Torre.

Results:

In the first year of the project, the focus has been on getting acquainted with state of the art research in the fields relevant for the project. This has been accomplished by conducting a study of the literature and by visiting a large number of conferences, workshops and research talks on the topics of games, security and logic. Furthermore, the research in attack–defense trees has led to a conference publication at GameSec’10 ([179]), and the research in solution concepts for game theory has led to a poster presentation at DGL’10 and a conference submission (notification pending).

Security Analysis Through Attack–Defense Trees	
Acronym	SADT
Reference	PHD-09-167
Head of Project	Prof. Dr. Sjouke Mauw
Funding	FNR-AFR, 106476€
Running Time	01/01/2010–31/12/2012

Members:

Sjouke Mauw, Patrick Schweitzer, Barbara Kordy, Saša Radomirović

Domain(s):

security, formal methods, attack trees, defense trees, attack-defense trees, security assessment

Partner(s):

- Telindus, Luxembourg
- Sintef, Norway
- TXT e-solutions, Italy
- Cybernetica, Estonia

Description:

The project *Security Analysis Through Attack–Defense Trees* (SADT) is part of the ATREES project. It aims to extend and unify attack trees, introduced by Bruce Schneier in 1999. The extension of attack trees will be achieved by adding defensive measures to attack trees to create Attack–Defense Trees (ADTrees). This will allow security analysts to include countermeasures into their analysis. The unification will be achieved by developing one coherent formal framework for ADTrees. This unification will facilitate the development of a software tool. This tool will encompass most existing attack tree approaches using only a single formalism.

More concretely, we will define a unified language for ADTrees, introduce several semantics arising from different mathematical disciplines and already existing attack tree approaches, and create a software tool that supports the work of security analysts. With the help of case studies provided by the several industry partners, different use cases will be examined. This will allow us to tailor and refine the language and semantics. It will also help us to improve the usability of the software tool.

The SADT project is a joint research project of the Interdisciplinary Centre for Security Reliability and Trust (SnT) and SaToSS.

Results:

- One publication [74] presented at FAST'10 describing the ADTree language as well as several semantics and attributes.
- One joint publication with the S-GAMES project [179], presented at GameSec'10, describing the relation between a subclass of games and ADTrees using a specific semantics and attribute.
- Corporation with Marc Pouly (SnT) to research the relation between ADTrees and knowledge compilation.
- Three case studies using ADTrees.

Security Protocols in Identity Management	
Acronym	SPIM
Reference	BFR07-103, TR-PHD BFR07-103, EXT-BFR07-103
Head of Project	Prof. Dr. Sjouke Mauw
Funding	BFR, FNR-AFR, 18000€+ 70984€+ 36379€
Running Time	01/10/2007–30/11/2011

Members:

Sjouke Mauw, Ton van Deursen, Saša Radomirović

Domain(s):

security protocols, RFID, formal verification, security properties

Description:

Nowadays, our identity is represented by an ever growing pile of paper and plastic documents such as passports, social security cards, bank cards, store loyalty cards, and company employee badges. Each of these items is backed

by an entry in an electronic database. With increasing frequency we are also being represented by so-called virtual identities, for instance when purchasing items in online stores, visiting social networking websites, or simply accepting a website's "cookies". We can create and abandon these virtual identities at will and even share them with others.

Identity management is the assignment, verification, and revocation of the privileges, rights, and duties of electronic and virtual identities. The increase in electronic and virtual identities over the years has been dramatic. As a consequence, today, identity management is recognized as an important and expensive business problem. The number of electronic and virtual identities per individual, however, will grow even larger, due to the continuing effort to connect and network every aspect of our lives.

The advancement of a technology promotes new possibilities, new applications, but also new threats. For example, the imminent pervasiveness of Radio-frequency identification (RFID) systems will make it possible to cheaply collect and cross-reference a vast amount of data in order to infer sensitive personal information. It is clear that the communication between RFID tags and RFID readers needs to be secure.

The primary objective of the proposed work is the design and verification of secure communication protocols related to identity management and with a view towards emerging technologies such as RFID. We intend to achieve this objective by developing advanced formal verification methods and implementing an automatic tool. This development requires a fundamental study of non-standard security properties, such as non-traceability and no-theft-of-service, and an extension of a formal model for modelling of physical tokens.

Results:

- One publication [195] presented at RFIDSec'10 describing results related to a recently proposed RFID protocol.
- One publication [170] presented at the PrimeLife 2010 summer school.
- One presentation at a seminar with results related to insider attacks on RFID protocols. A paper about the topic is currently in preparation.

Cryptanalysis of Hash Functions	
Acronym	CRHF
Reference	TR-PHD-BFR07-031
Head of Project	Prof. Dr. Alex Biryukov
Funding	FNR-AFR PhD, 109€ per year
Running Time	01/05/2007 – 28/02/2011

Members: Ivica Nikolic

Domain(s): Cryptography

Description:

The goal of this project is to study design and cryptanalysis of cryptographic hash functions. Cryptographic hash functions are central primitives used as building blocks in most of security protocols. They provide data integrity (both in storage and in transit), are used in digital signatures, user identification (e.g. remote access), and are closely related to MACs (message authentication codes).

Results:

The following papers have been published in 2010:

- “Rotational Cryptanalysis of ARX ” (FSE 2010) [110]
- “Automatic Search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers: Application to AES, Camellia, Khazad and Others ” (EUROCRYPT 2010) [109]
- “Rotational Rebound Attacks on Reduced Skein” (ASIACRYPT 2010) [108]

Refining Key Components in Trust Models	
Acronym	RKCTM
Reference	TR-PDR BFR08-038
Head of Project	Prof. Dr. Sjouke Mauw
Funding	FNR-AFR Postdoc, 50360€ per year
Running Time	01/01/2009–31/07/2010

Members:

Sjouke Mauw, Baptiste Alcalde

Domain(s):

trust, recommender systems, formal methods

Partner(s):

ICR group

Description:

Trust is a prediction of reliance on an action, based on what one party knows about another party. The fundamental problem in trust management concerns the establishment of a trust relation in a virtual environment. A trust model attempts to quantify trust by combining relevant information from various sources.

The main aim of the present project was to investigate two research areas, namely delegation and competence, in the scope of a recently developed trust model. A wide variety of practical applications can be foreseen in domains such as e-banking services, spam filters, personal health records, and online communities. We also established a new area of research in solving decision problems based on risk and trust.

Results:

Two goals of the project were successfully fulfilled: the first was to build a framework for decision problems involving trust and risk, the second was to build formal foundations for trust delegation. The two other objectives were not fulfilled (Trusted Proof Carrying Code and trust framework applied to banking operations). However, we studied three other important aspects of trust management systems instead. First, we formalized the notion of Trusted Third Party (TTP), and proposed algorithms to ensure a fair choice of a TTP in various settings [154]. Second, we studied the incorporation of the trust component into a distributed voting scheme applied to Facebook publications [162]. Third, we refined one of the component needed in the decision problem, namely conviviality, and more precisely how to measure it. The corresponding research paper *How to measure the conviviality of a dependence network*, by Baptiste Alcalde, Patrice Caire, Leon van der Torre, and Chattrakul Sombattheera, has been accepted for publication at AAMAS'11.

Analysis of the SHA-3 Remaining Candidates	
Acronym	SHARC
Reference	F1R-CSC-AFR-080000
Head of Project	Prof. Dr. Alex Biryukov
Funding	FNR-AFR Postdoc, 102,620€
Running Time	15/10/2010 – 14/10/2012

Members: Gaëtan Leurent

Domain(s): Cryptography, Secret Key, Hash Functions, Cryptanalysis, SHA-3

Description:

This project is about the analysis of hash functions, and will be closely related to the SHA-3 competition currently run by NIST. In cryptography, a hash function is a public function with no structural properties. It is an essential primitive in modern cryptography, used in many protocols and standards, including signatures schemes, authentication codes, and key derivation.

Following devastating attacks against many widely used hash functions (including MD4, MD5 and SHA-1), NIST organized the SHA-3 competition to select and standardize a new hash function. This competition is similar to the AES competition held in 1998-2000, and attracts worldwide attention, with a large effort underway to assess the security of the candidates. During this project, we will study the application of known cryptanalysis techniques to the new designs submitted for the SHA-3 competition, and try to develop new dedicated techniques tailored to some of the SHA-3 candidates.

Results:

The paper “Practical Partial-Collisions on the Compression Function of BMW” is accepted for presentation at the 18th IACR Workshop on Fast Software Encryption (FSE 2011).

Secure and Private Location Proofs: Architecture and Design for Location-Based Services	
Acronym	SECLOC
Reference	794361
Head of Project	Prof. Dr. Sjouke Mauw
Funding	FNR-AFR PhD, 109137€
Running Time	01/08/2010–31/07/2013

Members:

Sjouke Mauw, Xihui Chen, Jun Pang, Gabriele Lenzini

Domain(s):

security and privacy, location based services, location proofs, formal verification, trustworthy services, security protocols

Partner(s):

itrust Consulting Luxembourg

Description:

Location-based services are rapidly growing, as mobile networks become increasingly pervasive and the use of mobile devices is getting more popular.

Location-based applications make use of the physical location of the mobile device to provide services that are customized to that location. To be effective, location-based services need trustworthy (secure and private) positioning data: this depends upon the technology, the components and the communication protocols employed for service composition and provision. For this reason, researcher effort has been devoted to addressing the problem of how to certify a physical location and of how to ensure that location information is secure, e.g., in term of data integrity, non-transferability, unforgeability, and non-repudiation. Meanwhile, users have their privacy concerns about how their location proofs are used: e.g., they want to control when and to whom they need to present such proofs (anonymity), or they do not want a service provider to trace them.

Both security and privacy are essential in the development of location proofs for location-based services. While in the literature most researchers only consider security or privacy in isolation, we will address the problem of how to securely provide a user's location while adhering to the need-to-know principle for all other involved parties, thereby satisfying also privacy requirements of the users.

We approach this challenge by analyzing the concepts and requirements for security and privacy in a location proof management system. We aim at an architecture addressing both security and privacy requirements. We will design security/cryptographic protocols which can be used as building blocks in implementing such architecture for a concrete application domain. The correctness of the developed protocols is guaranteed through formal verification. At last, an experimental system based on the proposed architecture and protocols will be built to validate our solutions w.r.t. the security and privacy requirements identified.

Results:

- Location Privacy Preservation: We focused on anonymity in Location-based vehicle services. Currently we are working on the design of a privacy preserving electronic toll pricing system.
- Location Assurance Service: We did security analysis of current localization techniques and systems.

Expressing Non-Functional Requirements in Declarative Executable Models	
Acronym	ENRDEM
Reference	N/A
Head of Project	Prof.Dr.Pierre Kelsen
Funding	FNR, BFR/AFR ,
Running Time	01/01/2008 - 31/05/2010

Members:

Qin Ma

Domain(s):

Model-driven software engineering, Formal semantics, Model composition

Description:

The context of this project is the model-centric approach within model-driven software development that aims at providing a model-based description of a system that is precise enough for generating the full implementation. In particular the case where the behavior of the system is expressed using a declarative language will be considered. The goal of the project is to develop approaches for representing non-functional requirements in systems that have been specified in this way. Current work in aspect-oriented programming and aspect-oriented modeling will be analyzed for its applicability to this problem. The analysis will be based on a formal semantics of the behavioral description language that will be developed in a preparatory phase, based on existing approaches for defining the semantics of programming languages and of software models.

The project is closely related to the MEDAL project that is to be carried out at the Laboratory for Advanced Software Systems of the University of Luxembourg and fits within the high priority area P1 "Security and Reliability" of the University.

Results:

- A new paper titled "Models within Models: Taming Model Complexity using the Sub-Model Lattice", co-authored with Pierre Kelsen and Christian Glodt, has been accepted for publication in the conference proceedings of ETAPS/FASE 2011, one of the top venues in the area of fundamental approaches to Software Engineering.
- A new paper titled "Specifying structural properties and their constraints formally, visually and modularly using VCL", co-authored with Nuno Amalio, Pierre Kelsen and Christian Glodt, has been ac-

cepted for publication in the conference proceedings of EMMSAD 2010.

- A new paper titled “Using VCL as an Aspect-Oriented Approach to Requirements Modelling”, co-authored with Nuno Amalio, Pierre Kelsen and Christian Glodt, has been accepted for publication in the journal of Transactions on Aspect Oriented Software Development.
- A new technical report titled “A Generic Model Decomposition Technique”, co-authored with Pierre Kelsen and Christian Glodt published by the Laboratory of Advanced Software Systems (LASSY) in the Computer Science and Communications Research Unit at the University of Luxembourg.

The project has successfully accomplished by the end of May 2010.

PRISMA : a Process for Requirements Identification, Specification and Machine-supported Analysis, targeting Transactional Models seen under a Product Line perspective

Acronym	PRISMA
Reference	N/A
Head of Project	Prof. Dr. Nicolas Guelfi
Running Time	16/03/2006 –15/03/2010

Members:

Barbara Gallina

Domain(s):

Computer Science, Software Engineering, Product Line, Transaction Processing

Partner(s):

University of Newcastle upon Tyne, School of Computing Science, UK

Description:

The objective of this research project consists in the provision of a requirements engineering process, called PRISMA, targeting a Software Product Line constituted of (Advanced) Transactional Models. PRISMA should provide a sharply focused approach and should benefit from the current best practices within the Software Product Line community. PRISMA should support the elicitation, specification and verification/validation activities during the domain engineering phase as well as the application engineering phase. The result of the PRISMA process should be a valid and correct

requirements specification of a transactional model, seen as a 'product' of the product line. This process should contribute on one hand in increasing quality, in particular dependability, and on the other hand in reducing time to market and cost by intensifying reusability. PRISMA should integrate those significant results achieved previously in the framework of this project (i.e. the requirements elicitation template targeting dependable Software Product Line, called DRET; the thorough analysis concerning commonalities and variabilities among transactional models, the specification language targeting transactional models, called SPLACID).

Results:

The current year has been devoted to the enhancement/integration of the results achieved in the previous years and to their coherent presentation. The result of this work is a PhD thesis, which was defended in April.

Selected Problems in Executable Modeling	
Acronym	SPEM
Reference	PHD-09-084
Head of Project	Prof. Dr. Pierre Kelsen
Funding	FNR-AFR PhD
Running Time	15/11/2009 – 15/11/2012

Members:

Moussa Amrani and Nuno Amalio

Domain(s):

Model-Driven Engineering, Domain-Specific Modeling Languages, Structural and Behavioural Specification, Structural and Behavioral Semantics, Executability

Description:

Model-Driven Engineering considers models as first-class entity in the development process. In this way, developers deal only with models, which are used at the required level of abstraction for each task they need to perform to finally generate actual code on a given platform.

Transformations can also be modeled. Transformations are the Model-Driven Engineering tool that allow one to make models change, evolve to finally compute something. Transformation Languages can be classified in two trends: *object-oriented* languages and *rule-based* languages. Each of them present some strengths, but comes with some complications when dealing with huge models and / or huge transformations.

The Model-Driven Engineering approach gained maturity over the years and started to be used for safety-critical and embedded softwares, where formal verification plays a key role in the validation of applications. Formal verification could be performed either by model-checking exhaustively the execution state space, or by theorem-proving assertions and properties about the execution states. But to be able to use such techniques, formal semantics of transformation languages must be precisely specified.

This PhD has three goals:

1. Define the semantics of a transformation language;
2. Equip a transformation language with the ability to define contracts, which are an abstract and adequate way of defining behavior without going into implementation details;
3. Apply theorem-proving techniques to formally verify models and transformations against dynamic properties.

Results:

Since the PhD started the last year, the results are just coming. The results basically follows the first workpackages defined in the AFR proposal. It is also important to mention participation in conferences and paper review for a PhD.

State of the Art in Model-Driven Engineering This year was largely dedicated to study the existing techniques and tools for structural and behavioral modeling. A Technical Report will be soon published on behalf of the LASSY/CSC addressing these points, and completed with the graph- based tools.

Semantics Specification of an Object-Oriented Transformation Language

An important result regarding the development of formal verification techniques over Domain-Specific Modeling Languages is the formal specification of the semantics of such languages. It is known to be a hard task, but it is a necessary step towards formal and trustable verification. In the next few months, an article paper will be published soon.

Conference / Summer School Participation The candidate participated to one important conference in the domain, namely the European Conference on Modeling Foundations and Applications (ECMFA 2010); and the First Summer School on Domain-Specific Modeling, Theory and Practice (DSM- TP 2010).

Reliable and robust management for telecommunication network with optimization techniques	
Acronym	R2MTO
Reference	TR-PHD BFR07-105
Head of Project	Prof. Dr. Pascal Bouvry
Funding	FNR - AFR PhD
Running Time	01/12/2008 – 30/11/2010

Members:

Julien Schleich

Domain(s):

mobile ad hoc network, virtual backbone, decentralized algorithm, global optimization

Partner(s):

University of Metz

Description:

Ad hoc networks are infrastructure-less spontaneous networks generally composed of wireless and mobile devices. From a practical point of view, ad hoc technologies offer solutions when infrastructure-based network are too costly, damaged or not suitable. Despite a wide panel of scenarios and the huge number of ad hoc capable devices currently in use, this technology is not widely used because of technical considerations mainly related to the lack of a global coordinator. We propose two different approaches to create virtual backbones in order to organize ad hoc networks: a centralized algorithm based on DC programming and DCA to solve the Min m -Vertex Dominating Set Problem, and two distributed and asynchronous algorithms, relying on 2-hop knowledge only, to build k -Vertex Connected m -Vertex Dominating Set-based Virtual Backbones.

Results:

This is a list that enumerates the results obtained until now:

- Two decentralized algorithms, Backbone1 and 2, for virtual backbones in ad hoc networks
- Quality measures for virtual backbones in mobile environment
- One centralized algorithm based on DC and DCA to compute the minimum m -vertex l -level dominating set of a graph

Two decentralized algorithms [70, 71] were proposed to create robust and reliable virtual backbones for mobile ad hoc network. In the literature, the quality quantification of such structures is most of the time considering only one aspect (i.e. the cardinality of the backbone nodes set). In order to encompass all the different and often antithetical quality aspects, we provide a set of quality measures for virtual backbones in mobile environment [184].

In a second part of our work, we adopted an Operational Research point of view to deal with the minimum m -vertex l -level dominating set problem, for we think that theoretical guaranties are important yet not sufficient when dealing with solving NP-Hard optimization problems. As a consequence, developing a near-optimal algorithm based on DC programming and DCA allowed us to test much bigger instances of graphs than what can usually be optimally solved. We empirically validated our algorithm and showed that it is more robust and efficient than the CPLEX solver from ILOG software via extensive tests on random graphs. Results have been submitted to the Journal of Combinatorial Optimization edited by Springer and are still in the review process.

This thesis has been defended on September 28, 2010, after exactly three years, and received the grade outstanding.

Trust Management for Ad-Hoc Networks	
Acronym	TMAHN
Reference	TR-PHD BFR05-037
Head of Project	Prof. Dr. Pascal Bouvry
Funding	FNR - AFR PhD
Running Time	01/02/2007 – 31/01/2011

Members:

Apivadee Piyatumrong

Domain(s):

Mobile Ad Hoc Networks, Virtual Backbone, Trust, Spanning Tree, Multi-Objective Optimization

Partner(s):

- University of Le Havre, France
- King Mongkut's University of Technology Thonburi, Thailand

Description:

Within the framework of confident management (trust), the emerging char-

acteristics of one of the new types of networks, Mobile Ad Hoc Network (a network which has high dynamic movement of participants and needs decentralized management system) will be studied. Indeed, the traditional management sciences of identification and of reputation do not adapt to a new generation of this self-organized networks. MANETs (mobile Ad Hoc Networks) nowadays benefit of a quite large literature. However, they are often restricted to a fully connected to a fully connected network operating on TCP-IP. We wished to have the opportunity to also address Delay Tolerant Networks (DTNs) that may be partitioned from time to time. Existing studies consider such partitions as a low layer concern similar to latency or as a high level concern by considering that a DTN consists of a set of separated structures that may latter on split or merge depending on the mobility and environment of the devices. Furthermore, the system should be emerged in distributed and mobile environments. Classical security mechanisms do not apply for such networks that need fully decentralized management schemes. This thesis proposes to explore new opportunities through the concept of reputation in dynamic environment.

Results:

This study aims at providing a framework of topology management (TM) that comprises of (1) a set of robust criteria for topology management problem, (2) a set of solution algorithms that are decentralized, asynchronous algorithms which utilize local knowledge, and (3) evaluation methodologies for different solutions of different problems (e.g., single-objective and multi-objective problem).

The framework is divided into three main sectors according to the components stated above.

- The robust criteria selected in this study are the trust level of cooperative enforcement paradigm, the available energy of entity and the capacity bandwidth of communication links. The combination of such criteria together for robust topology management problem is a novelty which has not been dealt with in literature to date.
- In the solution phase, this study implements G-NODE, G-PATH, G-Node-Path, DFSmove, BREAK, and CHANCE heuristic as solutions of the framework. These algorithms and heuristics are totally decentralized and use only one-hop information. The decision is made locally without any consultation with other nodes.
- In the final phase of this framework, simulation programs and methodologies are prepared for evaluating the proposed algorithms based on different aspects to the problem. The evaluation phase is done offline and global information is assumed.

This thesis has been defended on December 17, 2010, and received the grade outstanding.

Confidentiality, Integrity issues in distributed computations	
Acronym	CIDC
Reference	N/A
Head of Project	Prof. Dr. Pascal Bouvry
Funding	FNR - AFR PhD
Running Time	01/01/2010 – 31/12/2012

Members:

Benoit Bertholon

Domain(s):

Confidentiality of execution, Integrity of execution, Cloud Computing, IaaS, Trusted Platform Modules, Parallel and Distributed Computing

Description:

Computing grids, as defined in [Fos97], are distributed infrastructures that gather thousands of computers geographically scattered and interconnected through the Internet. A simple concept that has emerged out of such an architecture is that of cloud computing (CC) where customers do not own or rent any part of the infrastructure. They simply use the available services and pay for what they use.

The CC paradigm currently arouse enthusiasm and interest from the private sector, because it allows to reduce computing cost at a time where computing power is primordial to reach competitiveness. Despite the initiative of several vendors to propose CC services (Amazon, Google etc.), several research questions remain open, especially as regards security aspect from the user point of view. CC highlights strong needs in integrity certifications and execution confidentiality, the latter focusing few academic interest until now. The current policy at this level is to blindly trust the vendor providing the CC service. This doesn't hold for critical applications that eventually use or generate sensitive data, especially when physical machines are distributed in different administrative domains and shared with other users that may be business competitors.

In the framework of the CC paradigm, the purpose of this PhD is therefore to investigate and design novel mechanisms to cover the following domains:

- **confidentiality** of both application code and user data;

- **integrity** and **fault-tolerance** to provide guarantees on programs and data, either before, during or after a run on the CC platform.

To make this study more concrete, the developed solutions must be validated on a CC platform build on top of the University of Luxembourg's computing clusters and the Grid5000 platform.

By addressing those issues, this PhD opens the perspective of intellectual patents in a key area able to address industrial needs in an emerging technology.

Results:

In the preliminary work, I studied the TPM; I read the documents issued by the Trusted Computing Group (TCG) regarding the specification of the TPM, as well as other papers using the TPM for different purposes. This has been done in order to develop what has been the main contribution of this first year: CertiCloud.

CertiCloud is a framework developed to verify the integrity of a running Virtual Machine in a Cloud environment. The creation of this prototype, based on a network communication protocol, developed and studied specifically for CertiCloud, forced me to get acquainted with protocol verification techniques.

Designing the network protocol is not the only work I have done on CertiCloud. I have also implemented it on a running machine, and performed experiments to determine the overhead of the verification of the Virtual Machine.

The second part of the PhD thesis concerning the Confidentiality of execution has started by the study of the work done by Dr. C. Gentry on fully homomorphic encryption scheme as well as obfuscation techniques classified by Prof. C. Collberg. This has been done in parallel with the work done on CertiCloud, previously described. This part is still in its early state, as i need to continue reading and understanding the literature. It will focus not only on how to obfuscate a program, but mainly how to measure the obfuscation of a program. The development of an adequate metric will be the most difficult part.

Combinatorial optimization on P2P systems and computational grids	
Acronym	COPSCG
Reference	TR-PHD BFR07-079
Head of Project	Prof. Pascal Bouvry
Funding	FNR - AFR PhD
Running Time	01/09/2007 - 31/10/2011

Members:

Malika Mehdi

Domain(s):

Combinatorial Optimization, Grid Computing

Partner(s):

University of Lille

Description:

The objectives of this PhD are the design of efficient hybridization schemes combining different kinds of optimization methods (exact methods and heuristics) and the design of a framework for large scale parallel optimization on computational grids to solve large benchmarks of permutation problems. The idea in this work is to re-use in metaheuristics, the tree-based representation of search spaces, that is generally used in exact optimization methods (like branch-and-bound) to enumerate all the solutions of the search space, in order to define a conceptual framework for the cooperation of optimization methods in a computational grid.

Results:

- A hybrid cooperative scheme combining an exact algorithm, the branch-and-bound algorithm (BandB), and genetic algorithms (GAs) is proposed to solve large scale permutation problems. Moreover, since this hybridization is CPU time intensive when applied to large permutation optimization problems, a hierarchical master-slave parallelization of this hybrid method is also proposed. This parallel method is adapted to the grid architecture and has been evaluated over the computational grid Grid'5000. In the experiments, a set of unsolved benchmarks of the 3D quadratic assignment problem (Q3AP), one of the hardest permutation-based problems, have been solved. New upper-bounds have been found for a set of unsolved Q3AP benchmarks and some of them have been proved to be optimal [104].

- Experiments are still in progress in order to solve a size 15 Q3AP benchmark using the parallel hybrid method GA-BandB (the largest Q3AP benchmark optimally solved in the literature is of size 14).
- A software framework for the cooperation of optimization methods (exact and metaheuristics) in a computational grid is developed.

Robust Scheduling on Desktop Grids	
Acronym	RSDG
Reference	PDR-08-010
Head of Project	Prof. Dr. Pascal Bouvry
Funding	FNR - AFR PostDoc
Running Time	01/09/2009 – 31/08/2011

Members:

Dr. Johnatan E. Pecero Sanchez

Domain(s):

Computer Science, Information Science, Grid Computing, Scheduling, Optimization

Description:

New distributed computing platforms (grids) are based on interconnections of a large number of processing elements. A most important issue for their effective utilization is the optimal use of resources through proper task scheduling. It consists of allocating the tasks of a parallel program to processors on the platform and to determine at what time the tasks will start their execution. As data may be subject to uncertainties or disturbances, it is practically impossible to precisely predict the input parameters of the task scheduling problem. The effects of uncertainties and/or disturbances on the data may impact system's efficiency, eventually leading either to infeasible situation, or to the generation of opportunities that improve its performance. Therefore, the problem is how to find a good schedule in such context. Thus it is essential to develop new mechanisms for controlling, and if necessary adjusting, the algorithm to guarantee reasonable performances.

Results:

The aim of this project is to study robust scheduling issues on grid computing systems. We concentrate on desktop grids. The objective is to design robust static scheduling algorithms that can behave well in presence of uncertainties or that are able to adapt their strategy due to bad estimations of parameters. The final goal is to contribute to the global efficiency of the

computations on Desktop Grids despite node heterogeneity, volatility and security mechanisms.

In parallel, we are investigating energy-efficiency issues on large-scale distributed systems. Energy-efficiency is a major concern in most of these systems (e.g. grids) since energy optimization brings various benefits, such as reducing monetary operating cost, increasing system reliability and reducing environmental impact. In this direction we started by developing and investigating models for processing elements in these computing systems. We summarize the models as follow:

Hierarchical Multi-core based systems [177]. Multi-core based systems [224]. We have also considered embedded systems. In this model, we consider a processor composed of several hierarchical functional units with incomplete bypass.

In the context of large-scale distributed systems we have studied a system composed of homogeneous processors with distributed memory and homogeneous network links [209]. Then, we have extended the model to homogeneous processors interconnected in an heterogeneous network[216]. Finally, we have considered scalable and distributed computing systems: Heterogeneous Processors Interconnected in an Homogeneous Network [93].

Efficient data transfer in vehicle2vehicle wireless communication networks, using distributed algorithms based on collective intelligence such as ant colonies.

Acronym	WiCaN
Reference	PDR-09-042
Head of Project	Prof. Dr. Pascal Bouvry
Funding	FNR - AFR PostDoc
Running Time	15/10/2009 – 14/10/2011

Members:

Yoann Pigné

Domain(s):

VANET, Distributed Computing, Routing Algorithms, Collective Intelligence, Ant-Based Algorithms, Multiobjective Optimization

Description:

Nowadays, safety efforts are more and more put into communications to prevent accidents rather than into safety devices and equipments (airbags, seat belts) to reduce the seriousness of accidents. New technology trends give

us wireless possibilities for mobile networking. These technologies can help in designing communication and warning systems needed with the help of vehicle-to-vehicle (V2V) communication. If we consider the communication network as a dynamic graph, routing in such a network can be reduced to finding and maintaining shortest paths in this graph, using only local information. We already successfully proposed a multiobjective algorithm based on ant colonies to find and maintain routes in a MANET. The proposal here is to apply this previous work to the special constraints of V2V networks and propose efficient data transmission algorithms with the help of artificial ants. Those methods will be tested and validated in realistic simulations, against other state of the art methods.

Results:

In the main purpose of producing realistic vehicular simulations, an integration of state of the art network simulator and vehicular traffic simulator has been investigated. The result of this work is a simulation platform dedicated to the communication between vehicles and infrastructures and also between vehicles themselves. Both simulators are coupled so that the mobility of vehicles in the traffic simulator is injected in the mobility model of the network simulator. Inversely, any simulated network application in the network simulator can influence the traffic simulation and, for instance, reroute simulated vehicles.

The platform can be used in any vehicular simulation environment. This work has been published [202] and is available online [here](#).

Following the same realistic simulation guidelines, the focus has then been put to the mobility of vehicles, and more precisely, to the one taking place in Luxembourg. Some sources of data proposed by the *Administration des Ponts et Chaussées* in Luxembourg allow the design of a mobility model that could simulate the commute traffic around the city of Luxembourg. This work is freely available [here](#). and a publication is accepted in the conference Nets4Cars 2011.

Additionally, unpublished work [228, 225] from my previous position have been presented in two international conferences, ALGOTEL 2010 and ANTS 2010.

Energy-Performance Optimization of the Cloud	
Acronym	EPOC
Reference	AFR MARP C09/IS/05
Head of Project	Prof. Dr. Pascal Bouvry
Funding	FNR - AFR PhD 108125.58 €.
Running Time	01/09/2010 – 31/08/2013

Members:

Frederic Pinel

Domain(s):

energy-efficiency, cloud computing

Partner(s):

NDSU, USA

Description:

This MARP PhD project, as part of the overall FNR CORE project Green-IT, will contribute to the solution of the energy efficiency in the following ways:

- Model the computing clouds, so that new methods can be designed to tackle the challenge. This involves mathematical analysis of the various parts of the cloud.
- Based on the models defined previously, design new algorithms (for example, from the fields of meta-heuristics and game theory) to energy-efficiently allocate resources of the cloud to client requests.
- Design methods for autonomic management of the cloud. Distributed agents will cooperate to allow the cloud to self-recover from any incident.
- Validate the implemented algorithms on large scale, real-world infrastructures. Both Grid 5000 and North Dakota State Data Centers are available for this step.

In addition to the theoretical contributions, this project will develop real software solutions.

Results:

The project began with the modeling of the basic components of a cloud: the individual servers. The multi-core, multi-processor, along with their main memory subsystem were studied [224]. Specifically, the impact of contention within these servers was modeled. Modern servers offer the abstracted view of a parallel machine: multi-processor and multi-core processors, time-sharing operating systems, scalar and hyperthreaded processors, contribute to this view. Yet significant contention exists within these servers, which impacts the theoretical expected performance.

Risk Prediction Framework for Interdependent Systems using Graph Theory	
Acronym	TIGRIS
Reference	PHD-09-103
Head of Project	Prof. Dr. Pascal Bouvry
Funding	FNR - AFR PhD
Running Time	15/10/2009 – 15/10/2012

Members:

Thomas Schaberreiter

Domain(s):

critical infrastructures, security modelling, graph modelling

Description:

Critical infrastructure protection is an up-to-date topic. Critical infrastructure is usually composed of interdependent systems that rely on each other in order to function correctly or provide adequate security. The interdependencies of the systems are usually quite complex to understand and therefore modelling of the infrastructure and its interdependencies can be helpful in determining the security requirements. During this work a model of interdependent systems based on graph theory will be proposed that aims to model the security attributes of interdependent systems. Adequate ways to model the security properties of infrastructure as well as of the interdependencies will have to be found in order to achieve a close-to-reality model. Furthermore, machine learning tools will have to be developed in order to process the graph and allow real-time simulations.

Results:

- State-of-the-art analysis in the areas critical infrastructure modelling, critical infrastructure simulation and risk in critical infrastructures
- Preparation of conference paper presented at ARES2010 conference ("Risk-Based Methodology for Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures" [10]).
- Preparation of conference paper presented at ESREL2010 conference ("Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures. Case study of a Risk-Based Approach." [9]).
- Preparation of workshop paper for RTTE2010 workshop ("Support tool development for real-time risk prediction in interdependent critical

infrastructures”, [8]).

- Work on conference paper dealing with a trust based approach for interdependency weighting (currently in conference review process).
- Work on conference paper dealing with dependency analysis in complex systems (currently in conference review process).

Towards a unified logical framework for action, uncertainty, and causality	
Acronym	ULFAUC
Reference	TR-PDR BFR08-056
Head of Project	Prof. Dr. Leon van der Torre
Funding	FNR-AFR-Postdoc
Running Time	01/09/2008 – 31/08/2010

Members:

Guillaume Aucher

Domain(s):

Knowledge representation, Logic, Causality

Description:

Reasoning adequately about actions and causality under uncertainty is an important issue that is relevant to many fields such as artificial intelligence, social sciences, economics, cognitive psychology, and engineering. This problem has only partly been tackled by declarative logic-oriented approaches. These have usually focused on just one of the relevant themes: action, causality, or uncertainty. Popular accounts include the situation calculus, dynamic epistemic logic, Pearl’s causal networks, and conditional logics. However, because these issues are closely related, they should preferably be addressed together. It is the goal of this project to contribute to the creation of such an integrated logical framework. Furthermore, we try to apply the techniques developed in this context also to open questions in normative reasoning.

Results:

- In [61], we have proposed a logical formalism that is able to represent the world during the occurrence of events. It models the fact that our perception of events, and not only that of the static situation, can be updated due to the occurrence of other events.

- We have axiomatized the standard update product of dynamic epistemic logic. This provides a natural characterization of this update and paves the way to a systematic study of updates [6].
- We have also modeled within a unified logical framework the classical distinction between prescriptive and descriptive obligation, addressing a long-standing problem of deontic logic [7].
- A logical framework has been proposed where norm change can be modeled based on a combination of Anderson's deontic logic and dynamic epistemic logic. We compared our approach with the AGM paradigm [60].
- We developed a logical approach to problems of privacy and confidentiality using a combination of deontic logic and dynamic epistemic logic [120].

Logic and Communication in Normative Multi-Agent Systems	
Acronym	LCNMAS
Reference	PDR-08-013
Head of Project	Prof. Dr. Leon van der Torre
Funding	FNR-AFR-Postdoc
Running Time	01/03/2009 – 28/02/2011

Members:

Xavier Parent

Domain(s):

Agent communication languages, Normative multi-agent systems, Deontic logic

Description:

The project's aim is to explore the use of deontic logic in the context of communication protocols in multi-agent systems, and to explore the fruitfulness of the Normative Multi-Agent System (NorMAS) approach to the Agent Communication Language (ACL). The project is constructed along two axes: whether the notion of commitment can be analyzed in terms of obligation; whether conversation rules or protocols can be described as soft rather than hard constraints.

Results:

- Axis 1: Commitment.

The focus is on the Alston notion of commitment. Traditional deontic logic systems make strong assumptions about the speaker's rationality. His preferences over dialogue moves are required to be total and transitive.

The first achievement is a completeness result for an axiomatization of a logic that relaxes these assumptions [19]. This problem has been left open for forty years in deontic logic.

The second achievement (joint work with Prof. D. Gabbay) is a 2-dimensional analysis of obligation. The two dimensions are used to model the distinction traditionally made between actual and ideal obligations. This gives a finer-grained analysis of commitment. What the speaker commits to might be held to depend on context, in the sense that it might be held to depend on whether another (primary) commitment is fulfilled or violated. This paper will be published in *Synthese*.

- Axis 2: Conversational rules.

The first achievement is a dialogue model based on iterated belief revision theory, explaining how obligations are updated as the dialogue evolves. Compared to other approaches, the main novelty consists in keeping open the possibility that an agent breaks the rules of the game.

The second achievement concerns the scope of the model. We extended the approach to allow conversational interactors to detect and resolve conflicts among rules. (The corresponding paper received the best paper award at DEON'10 [130]). The main hypothesis is that violation and conflict detection are intimately intertwined. This motivates the use of an umbrella formalism (input/output logic) covering both aspects. My joint chapter with Prof. Dr. van der Torre on input/output logic for the *Handbook of Deontic Logic* laid the groundwork for this research [5]. The chapter provides an overview of input/output logic as a framework for reasoning about norms.

Implementation of Formally Well-Founded Graph Transformations on the Resource Description Framework with Applications to Domain-Specific Modelling Languages	
Acronym	RDFGraTra
Reference	PDR-09-066
Head of Project	Prof. Dr. Thomas Engel
Funding	FNR - AFR PostDoc - 52817€
Running Time	2010–2011

Members: Thomas Engel, Benjamin Braatz

Domain(s): Domain-Specific Modelling

Description: The two main aims of this project are the realisation of an algebraic graph transformation engine for the Resource Description Framework (RDF) and a case study on using this engine for managing domain-specific models from a family of interconnected modelling languages.

RDF provides the fundamental data structures for the Semantic Web. It allows to store distributed, machine-interpretable information in data stores based on a graph-like abstract syntax.

Algebraic graph transformations are a formal model for rule-based modifications of graph-like structures which allow the definition of languages by grammars, the creation of complex modification rules by composition of smaller rules and the reasoning about dependencies and independence of transformations and confluence and termination of sets of transformation rules.

By implementing a graph transformation engine on RDF we obtain, on the one hand, a modification mechanism with a rich theoretical background which is not available up to now. On the other hand, this implementation allows to carry out graph transformations on large data stores which is not possible with today's graph transformation engines.

Domain-specific modelling languages (DSMLs) are used today to facilitate code generation from small languages tailored to the needs of specific user groups. In contrast to that, this project focusses on families of interconnected DSMLs tailored to several groups of users. In a case study such a family shall be defined using RDF graph grammars and the evolution of domain-specific models and the integration of models from different DSMLs shall also be achieved by RDF graph transformation rules.

Moreover, we want to show how the knowledge about best practices w. r. t. the aspects of the world modelled in the DSMLs can be encoded using graph transformation rules.

Results: Results concerning the adaptation of graph transformation theory to RDF graphs and other relational structures have been published in [26]

and [114]. A first paper on the integration of graph transformations into the existing landscape of the Semantic Web has been published in [113]. A case study on the application of RDF graph transformations to DSML families with use cases for language evolution and migration and integration of several DSMLs has been presented at the International Conference on Software Language Engineering and will appear in the corresponding proceedings.

Energy Optimization and Monitoring in Wireless Mesh Sensor Networks	
Acronym	WiNSEOM
Reference	N/A
Head of Project	Prof. Dr. Thomas Engel
Funding	FNR - AFR PhD - 36042 €/year
Running Time	01/09/2010 – 31/08/2013

Members:

David Fotue, Thomas Engel, Houda Labiod, Foued Melakessou, Sunil Kumar and Prasant Mohapatra

Domain(s):

Wireless Sensor Networks

Partner(s):

- Telecom ParisTech, France
- University of San Diego, USA
- University of California Davis, USA
- Ville du Luxembourg
- Service de Coordination Hotcity

Description:

Air pollution is now considered as an important issue that needs to be treated as a critical phenomenon. It belongs to a set of crucial physical factors that drastically decrease people's health of human beings. In this proposal, we aim to deploy an efficient monitoring architecture dedicated to Air Pollution in Luxembourg based on Wireless Sensor Networks (WSNs). WSNs have been the subject of much recent study and are a potential solution for the deployment of measurement architectures at low cost. They allow the measurement of data and their transmission towards a central workstation, often called the sink, in an efficient manner. Currently, air pollution monitoring is done locally over a small area. The deployment of a large set of

sensors enables better mapping of pollution occurrences at a higher measurement frequency. Optimal communication in WSNs is currently a hot research topic. For instance, during the last ten years researchers have suggested many routing protocols in order to optimize data transfer between network nodes. We propose new routing protocols and forwarding mechanisms that increase network lifetime, through the set of route diversity and efficient energy management schemes. A set of maximally disjoint paths between each sensor and the sink can partially or completely avoid the appearance of congestion in the network. The residual energy of sensors is also taking into account our model. Consequently, data packets will be forwarded towards candidates that present the widest capabilities and have the greatest residual energy. Consequently, global traffic will be spread along non-overlapping paths in order to increase the global WSN lifetime. The PhD work consists of the analysis of this energy routing protocol, in the case of a real scenario that will be deployed in Luxembourg for air pollution analysis.

Results:

After a study of the state of the art in the area of WSNs for energy optimization, we proposed: A new Energy Conserving Routing Protocol that aims to optimize the transmission cost over a path from a source to a defined destination in a Wireless Sensor Network. The results appears in proceedings of the 9th IEEE/IFIP Annual Mediterranean Ad Hoc Networking Workshop, France, 2010. New Aggregation Techniques for Wireless Sensor Networks have been proposed, the results appears in proceedings of the 18th Annual Meeting of the IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems(MASCOTS), USA, 2010. 3. We study the effect of Sink Location on Aggregation based on Degree of connectivity for Wireless Sensor Networks. The results are under reviews at the First International Workshop on Advanced Communication Technologies and Applications to Intelligent transportation systems, Cognitive radios and Sensor networks(ACTIS), Korea, 2011. 4. We proposed a new Hybrid method to assign the channel for Wireless Sensor Networks. The results are under reviews at the 9th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks(WiOpt), USA, 2011. 5. Finally, we concluded all investigations done this year by submitting a journal paper at EURASIP Journal on Wireless Communications and Networking, in the special issue "Localization in Mobile Wireless and Sensor Networks."

4.2.2 Workshop & Conferences (FNR Accompanying Measures)

ESC 2010 - Early Symmetric Cryptography Workshop	
Acronym	ESC 2010
Reference	F1C-CSC-PMA-090314
Head of Project	Prof. Dr. Alex Biryukov
Funding	FNR-AM3, 8000€
Running Time	11/01/2010 - 15/01/2010

Members:

Ralf-Philipp Weinmann

Domain(s):

Symmetric Cryptography

Description:

ESC is a five-day Dagstuhl-like seminar organized by LACS that took place in January 2010 in Remich, Luxembourg.

Results:

More than 40 leading experts in symmetric cryptography attended ESC 2010 and gave talks on their most recent research in the area of symmetric cryptography and algorithmic challenges in cryptography. ESC 2010 continued the series of seminars on symmetric cryptography that took place at Dagstuhl 2007, 2009 and Echternach 2008. The program of ESC 2101 is available online at https://cryptolux.org/ESC/Seminar_program.

CSC Representation

5.1 Conferences

The following local events have been organized during 2010:

- **OPTIM 2010 Workshop**, Workshop on optimization issues in energy efficient distributed systems, 28/06/2010 - 02/07/2010, Caen, France, Prof. Dr. Pascal Bouvry, Dr. Grégoire Danoy, Dr. Bernabé Dorronsoro, Dr. Sébastien Varrette (organizers)
- **Special Session on Metaheuristics for Green Computing** in META 2010, 27/10/2010 - 31/10/2010, Djerba, Tunisia, Prof. Dr. Pascal Bouvry (session chair)
- **BNAIC 2010 Conference**, 22nd Benelux Conference on Artificial Intelligence, 25-26/10/2010, Luxembourg, Prof. Dr. Pascal Bouvry, Prof. Dr. Leon van der Torre (general chairs)
- AI Lecture Series, Vol. III - Data Mining Applications (2010), University of Luxembourg, 26/10/2010 - 07/12/ 2010, Prof. Dr. Christoph Schommer (Conference Chairman)
- RuleML 2010 - 4th International Web Rule Symposium; Oct 21-23 2010; Washington, DC; USA; Antonios Bikakis (Area Chair)
- NMR 2010 - 13th International Workshop on Non-monotonic Reasoning - Action and Belief Change sub-workshop; May 14-15 2010; Toronto; Canada; Richard Booth (Sub-workshop chair)

- MIWAI 2010 - 4th Mahasarakham International Workshop on Artificial Intelligence; Dec 9-10 2010; Mahasarakham; Thailand; Richard Booth (PC chair)
- BNAIC 2010 - 22nd Benelux Conference on Artificial Intelligence; Oct 25-26 2010; Luxembourg; Luxembourg; Leon van der Torre (General chair), Richard Booth (PC chair)
- 10th Augustus De Morgan Workshop on Deontic Logic; Jul 5-6 2010; Florence; Italy; Leon van der Torre (Chair), Xavier Parent (Organizer)
- ESSLLI 2010 student session; Aug 9-20; Copenhagen; Denmark; Marija Slavkovic (Chair)
- LIS 2010: ESSLLI 2010 Workshop Logics in Security; Aug 9-13 2010; Copenhagen; Denmark; Dov Gabbay (Chair), Leon van der Torre (Workshop chair)
- NMR 2010 - 13th International Workshop on Non-monotonic Reasoning - Preferences and Norms sub-workshop; Jul 14-15 2010; Toronto; Canada; Leon van der Torre (Sub-workshop chair)
- WLIAMAS 2010 - 3rd Workshop on Logics for Intelligent Agents and Multi-Agent Systems; Aug 31 - Sep 3 2010; Toronto; Canada; Leon van der Torre (PC chair)
- CLIMA 2010 - 11th International Workshop on Computational Logic in Multi-Agent Systems; Aug 16-17 2010; Lisbon; Portugal; Wojciech Jamroga (Chair of special track)
- LAMAS 2010 - 3rd Workshop on Logical Aspects of Multi-Agent Systems; May 11 2010; Toronto; Canada; Wojciech Jamroga (Workshop organizer, PC co-chair), Matthijs Melissen (Workshop organizer)
- SERENE 2010 - 2nd International Workshop on Software Engineering for Resilient Systems, Birkbeck College, 13-16/04/2010, London, United Kingdom; Prof. Dr. Nicolas Guelfi (Steering committee co-chair)
- **Codebreakers 2010**, Luxembourg, 28-29/06/2010, Luxembourg, Prof. Dr. Peter Ryan (Conference Chair)
- **ESC 2010**, Early Symmetric Crypto seminar, 11-15/01/2010, Prof. Dr. Alex Biryukov (Program chair)

5.2 PC and other memberships

- **BNAIC 2010**, October 2010, Luxembourg, Pascal Bouvry (General co-Chair)
- **OPTIM 2010**, July 2010, Caen, France, Pascal Bouvry (General co-Chair)
- **META 2010**, October 2010, Djerba, Tunisia, Pascal Bouvry (Session Organiser)
- **ALIO-INFORMS 2010**, June 2010, Buenos Aires, Argentina, Pascal Bouvry (Session Organiser)
- **IHM 2010**, September 2010, Luxembourg, Pascal Bouvry (Session Organiser)
- **CEC 2010**, September 2010, Barcelona, Spain, Pascal Bouvry (Session Chair)
- **PPSN 2010**, September 2010, Gdansk, Poland, Pascal Bouvry (PC Member)
- **GECCO 2010**, July 2010, Portland, USA, Pascal Bouvry (PC Member)
- **AICCSA 2010**, May 2010, Hammamet, Tunisia, Pascal Bouvry (PC Member)
- **MENS '10**, December 2010, Miami, USA, Grégoire Danoy (PC Member)
- **BNAIC 2010**, October 2010, Luxembourg, Grégoire Danoy (PC Chair)
- **BNAIC 2010**, October 2010, Luxembourg, Marcin Seredynski (PC Chair)
- **OPTIM 2010**, July 2010, Caen, France, Grégoire Danoy (General Co-Chair)
- **ICUMT 2010**, October 2010, Moscow, Russia, Grégoire Danoy (PC Member)
- **WPS 2010**, December 2010, Miami, USA, Grégoire Danoy (PC Member)
- **GreenCom 2010**, December 2010, Hangzhou, China, Grégoire Danoy (PC Member)
- **IWSN 2010**, June 2010, Santa-Barbara, USA, Grégoire Danoy (PC Member)

- **IHM 2010**, September 2010, Luxembourg, Grégoire Danoy (PC Member)
- **TIDIAD 2010** - Workshop on Theories of Information Dynamics and Interaction and their Application to Dialogue, Aug 16-20 2010, Copenhagen, Denmark, Guillaume Aucher (PC member)
- **NMR 2010** - 13th International Workshop on Non-monotonic Reasoning - Action and Belief Change sub-workshop, May 14-15 2010, Toronto, Canada, Guillaume Aucher (PC member)
- **BNAIC 2010** - 22nd Benelux Conference on Artificial Intelligence, Oct 25-26 2010, Luxembourg, Luxembourg, Guillaume Aucher (PC-member)
- **AAAI 2010** - 24th AAAI Conference on Artificial Intelligence, Jul 11-15 2010, Atlanta, USA, Richard Booth (PC member)
- **ARCOE 2010** - Workshop on Automated Reasoning about Context and Ontology Evolution, Aug 16-17 2010, Lisbon, Portugal, Richard Booth (PC member)
- **ECAI 2010** - 19th European Conference on Artificial Intelligence, Aug 16-20 2010, Lisbon, Portugal, Richard Booth (PC member)
- **NonMon@30** - Thirty Years of Nonmonotonic Reasoning, Oct 22-25 2010, Lexington, USA, Richard Booth (PC member)
- **AI 2010** - 23rd Australasian Joint Conference on Artificial Intelligence, Dec 7-10 2010, Adelaide, Australia, Richard Booth (PC member)
- **ECAI 2010** - 19th European Conference on Artificial Intelligence, Aug 16-20 2010, Lisbon, Portugal, Martin Caminada (PC-member)
- **BNAIC 2010** - 22nd Benelux Conference on Artificial Intelligence, Oct 25-26 2010, Luxembourg, Luxembourg, Martin Caminada (PC-member)
- **COMMA** - 3rd International Conference on Computational Models of Argument, Sep 8-10 2010, Desenzano del Garda, Italy, Martin Caminada (PC-member)
- **COMMA** - 3rd International Conference on Computational Models of Argument, Sep 8-10 2010, Desenzano del Garda, Italy, Dov Gabbay (PC member)
- **DEON 2010** - 10th International Conference on Deontic logic in Computer Science, Jul 7-9 2010, Florence, Italy, Xavier Parent (PC member)

- Agent Communication 2010, May 11, 2010, Toronto, Canada, Xavier Parent (PC member)
- NORMAS 2010 - 5th International Workshop on Normative Multi-Agent Systems, Mar 29-30 2010, Leicester, UK, Gabriella Pigozzi (PC member)
- EC-Web-2010 - 11th International Conference on Electronic Commerce and Web Technologies, Aug 30 - Sep 3 2010, Bilbao, Spain, Gabriella Pigozzi (PC member)
- CLIMA 2010 - 11th International Workshop on Computational Logic in Multi-Agent Systems, Aug 16-17 2010, Lisbon, Portugal, Gabriella Pigozzi (PC member)
- BNAIC 2010 - 22nd Benelux Conference on Artificial Intelligence, Oct 25-26 2010, Luxembourg, Luxembourg, Gabriella Pigozzi (PC-member)
- ABC:MI 2010 - 7th Workshop on Agent-Based Computing: from Model to Implementation, Oct 18-20 2010, Wisla, Poland, Marija Slavkovic (PC member)
- KR 2010 - 12th International Conference on the Principles of Knowledge Representation and Reasoning, May 9-13 2010, Toronto, Canada, Leon van der Torre (PC member)
- ECAI 2010 - 19th European Conference on Artificial Intelligence, Aug 16-20 2010, Lisbon, Portugal, Leon van der Torre (PC member)
- AAMAS 2010 - AAMAS-2010, 9th International Conference on Autonomous Agents and Multiagent Systems, May 10-14 2010, Toronto, Canada, Leon van der Torre (PC member)
- DEON 2010 - 10th International Conference on Deontic logic in Computer Science, Jul 7-9 2010, Florence, Italy, Leon van der Torre (PC member)
- COMMA - 3rd International Conference on Computational Models of Argument, Sep 8-10 2010, Desenzano del Garda, Italy, Leon van der Torre (PC member)
- ESSLLI 2010 Workshop Theories of information dynamics and interaction and their application to dialogue, Aug 16-20 2010, Copenhagen, Denmark, Leon van der Torre (PC member)
- CLIMA 2010 - 11th International Workshop on Computational Logic in Multi-Agent Systems, Aug 16-17 2010, Lisbon, Portugal, Leon van der Torre (PC member)

- ARGMAS 2010 - 7th International Workshop on Argumentation in Multi-Agent Systems, May 10 2010, Toronto, Canada, Leon van der Torre (PC member)
- RuleML 2010 - 4th International Web Rule Symposium, Oct 21-23 2010, Washington, DC, USA, Leon van der Torre (PC member)
- COIN@AAMAS 2010 - Coordination, Organization, Institutions and Norms in Multi-Agent Systems, May 10-11 2010, Toronto, Canada, Leon van der Torre (PC member)
- COIN@MALLOW 2010 - 11th International Workshop on Coordination, Organization, Institutions and Norms in Multi-Agent Systems, Aug 30-Sep 2 2010, Lyon, France, Leon van der Torre (PC member)
- NORMAS 2010 - 5th International Workshop on Normative Multi-Agent Systems, Mar 29-30 2010, Leicester, UK, Leon van der Torre (PC member)
- PROMAS 2010 - 8th International Workshop on Programming Multi-Agent Systems, May 11 2010, Toronto, Canada, Leon van der Torre (PC member)
- LADS 2010 - 3rd International Workshop on Languages, Methodologies and Development Tools for Multi-agent Systems, Aug 31 - Sep 1 2010, Toronto, Canada, Leon van der Torre (PC member)
- PRIMA 2010 - 13th International Conference on Principles and Practice of Multi-Agent Systems, Nov 12-15 2010, Kolkata, India, Leon van der Torre (PC member)
- SNAMAS 2010, Mar 29 - Apr 1 2010, Leicester, UK, Leon van der Torre (PC member)
- SS@EASSS 2010 - Student session of the 12th European Agent Systems Summer School, Aug 23-27 2010, Lyon, France, Leon van der Torre (PC member)
- MIWAI 2010 - 4th Mahasarakham International Workshop on Artificial Intelligence, Dec 9-10 2010, Mahasarakham, Thailand, Leon van der Torre (PC member)
- WebKR3 2010 - International Workshop on Web-scale Knowledge Representation, Retrieval, and Reasoning, Aug 31 2010, Toronto, Canada, Leon van der Torre (PC member)
- ICAART 2010 - 2nd International Conference on Agents and Artificial Intelligence, Jan 22-24 2010, Valencia, Spain, Leon van der Torre (PC member)

- AICCSA 2010 - 8th ACS/IEEE International Conference on Computer Systems and Applications, May 16-19 2010, Hammamet, Tunisia, Leon van der Torre (PC member)
- ECAI 2010 - 19th European Conference on Artificial Intelligence, Aug 16-20 2010, Lisbon, Portugal, Emil Weydert (PC-member)
- BNAIC 2010 - 22nd Benelux Conference on Artificial Intelligence, Oct 25-26 2010, Luxembourg, Luxembourg, Emil Weydert (PC-member)
- NMR 2010 - 13th International Workshop on Non-monotonic Reasoning - NMR and Uncertainty sub-workshop, May 14-15 2010, Toronto, Canada, Emil Weydert (PC-member)
- ICAART 2010 - 2nd International Conference on Agents and Artificial Intelligence, Jan 22-24 2010, Valencia, Spain, Wojciech Jamroga (PC member)
- AAMAS 2010 - AAMAS-2010, 9th International Conference on Autonomous Agents and Multiagent Systems, May 10-14 2010, Toronto, Canada, Wojciech Jamroga (PC member)
- CoopMAS-2010 - 1st Workshop on Cooperative Games in Multiagent Systems, May 10 2010, Toronto, Canada, Wojciech Jamroga (PC member)
- LAMAS 2010 - 3rd Workshop on Logical Aspects of Multi-Agent Systems, May 11 2010, Toronto, Canada, Wojciech Jamroga (Co-organizer and PC co-chair)
- IIS 2010 - International Joint Conference Security and Intelligent Information Systems, Jun 8-10 2010, Siedlce, Poland, Wojciech Jamroga (PC member)
- LIS 2010: ESSLLI 2010 Workshop Logics in Security, Aug 9-13 2010, Copenhagen, Denmark, Wojciech Jamroga (PC member)
- ESSLLI 2010 student session, Aug 9-20, Copenhagen, Denmark, Wojciech Jamroga (PC member)
- STAIRS 2010 - 5th European Starting AI Researcher Symposium, Aug 16-20 2010, Lisbon, Portugal, Wojciech Jamroga (PC member)
- ECAI 2010 - 19th European Conference on Artificial Intelligence, Aug 16-20 2010, Lisbon, Portugal, Wojciech Jamroga (PC member)
- EC-Web-2010 - 11th International Conference on Electronic Commerce and Web Technologies, Aug 30 - Sep 3 2010, Bilbao, Spain, Wojciech Jamroga (PC member)

- LADS 2010 - 3rd International Workshop on Languages, Methodologies and Development Tools for Multi-agent Systems, Aug 31 - Sep 1 2010, Toronto, Canada, Wojciech Jamroga (PC member)
- WLIAMAS 2010 - 3rd Workshop on Logics for Intelligent Agents and Multi-Agent Systems, Aug 31 - Sep 3 2010, Toronto, Canada, Wojciech Jamroga (PC member)
- BNAIC 2010 - 22nd Benelux Conference on Artificial Intelligence, Oct 25-26 2010, Luxembourg, Luxembourg, Wojciech Jamroga (PC member)
- EUMAS 2010 - 8th European Workshop on Multi-Agent Systems, Dec 16-17 2010, Paris, France, Wojciech Jamroga (PC member)
- CogSci 2010 - The Annual Meeting of the Cognitive Science Society. Portland, USA, Prof. Dr. Christoph Schommer (PC Membership)
- AICCSA 2010 - 8th ACS/IEEE International Conference on Computer Systems and Applications, May 16-19, 2010, Hammamet, Tunisia, Prof. Dr. Christoph Schommer (PC Membership)
- CBMS 2010 - 23rd IEEE Conference on Computer-Based Medical Systems. Perth, Australia, Prof. Dr. Christoph Schommer (PC Membership)
- ICNC 2010 - 6th IEEE Conference on Natural Computation, Yantai, China, Prof. Dr. Christoph Schommer (PC Membership)
- ICNC 2010 - International Conference on Neural Computation, Valencia, Spain, Prof. Dr. Christoph Schommer (PC Membership)
- BNAIC 2010 - Benelux Conference on Artificial Intelligence, 2010, Luxembourg, Prof. Dr. Christoph Schommer (PC Membership)
- First Luxembourg-Polish Workshop on Security and Trust. Bourglinster Castle, Luxembourg, Prof. Dr. Christoph Schommer (PC Membership)
- IPTComm 2010 - Principles, Systems and Applications of IP Telecommunications 2010, Chicago, USA, Radu State (Steering Committee member)
- AIMS 2010 - 4th International Conference on Autonomous Infrastructure, Management and Security, Zurich, Switzerland, Radu State (PC member)
- NOMS 2010 - IEEE/IFIP Network Operations and Management Symposium, Osaka, Japon, Radu State (PC member)

- NEMA 2010 - Network Embedded Management and Applications, Osaka, Japon, Radu State (PC member)
- CNSM 2010 - International Conference on Network and Service Management, Niagara Falls, Canada, Radu State (PC member)
- Malware 2010 - 5th IEEE International Conference on Malicious and Unwanted Software, Nancy, France, Thomas Engel (PC member)
- **BENEVOL 2010** - BELgian-NEtherlands software eVOLution seminar; 16-17 December, 2010; Lilles ; France ; Pierre Kelsen (PC member)
- **3rd Workshop on Security and Trust**; January 2010; Luxembourg ; Pierre Kelsen (PC member, session chair)
- ISSRE 2010 - 21st annual International Symposium on Software Reliability Engineering; November 2010 ; San Jose ; USA; Nicolas Guelfi (PC member)
- PNSE'10 - International Workshop on Petri Nets and Software Engineering; satellite event of Petri Nets 2010 - 31st International Conference on Application and Theory of Petri Nets and Other Models of Concurrency ; June 2010 ; Braga; Portugal; Nicolas Guelfi (PC member)
- QUATIC'10 - 7th International Conference on the Quality of Information and Communications Technology - track on Quality in ICT Verification and Validation ; September 2010 ; Oporto; Portugal; Nicolas Guelfi (PC member)
- SEAFOOD 2010 - Software Engineering Approaches for Offshore and Outsourced Development - 4th International Conference; June 2010 ; St. Petersburg; Russia; Nicolas Guelfi (PC member)
- Modevva 2010 - The 7th workshop on model-driven engineering, verification, and validation, October 2010, Yves Le Traon (PC member)
- ICST 2010 - Third IEEE International Conference on Software Testing, Verification and Validation, Yves Le Traon (PC member)
- Mutation 2010 - 5th IEEE International Workshop on Mutation Analysis, Yves Le Traon (PC member)
- NEPTUNE'2010 - 7th NEPTUNE Annual Conference on Model-Driven Engineering: MDE & Embedded Systems, Yves Le Traon (PC member)

- AFADL 2010 - 10es Journées Francophones Internationales sur les Approches Formelles dans l'Assistance au Développement de Logiciels, Yves Le Traon (PC member)
- SEAA 2010 36th EUROMICRO Conference on Software Engineering and Advanced Applications, EDISON Track, September 2010, Lille, France, Jacques Klein (PC member)
- AOSD 2010 - Meta-Aspect 2010- International Workshop on Aspect-Oriented Meta-Modeling, March 2010, Saint-Malo, France, Jacques Klein (PC member)
- ESC 2010 , Alex Biryukov (Program chair)
- SAC 2010, Alex Biryukov (Program chair)
- FSE 2010, Alex Biryukov (PC member)
- CT-RSA 2010, Alex Biryukov (PC member)
- ACNS 2010, Alex Biryukov (PC member)
- WISSEC 2010, Alex Biryukov (PC member)
- ICICS 2010, Alex Biryukov (PC member)
- ICISC 2010, Alex Biryukov (PC member)
- ECRYPT Tools for Cryptanalysis 2010, Alex Biryukov (PC member)
- Codebreakers 2010, Alex Biryukov (PC member)
- EUROCRYPT 2010, Jean-Sebastien Coron (PC member)
- ASIACRYPT 2010, Jean-Sebastien Coron (PC member)
- SCN 2010, Jean-Sebastien Coron (PC member)
- CHES 2010, Jean-Sebastien Coron (PC member)
- PKC 2010, Jean-Sebastien Coron (PC member)
- IPSEC 2010 ,David Galindo (PC member)
- NSS 2010, David Galindo (PC member)
- EuroPKI 2010, David Galindo (PC member)
- ICISC 2010, David Galindo (PC member)
- ACSA 2010, David Galindo (PC member)

- CHES 2010, Johann Großschadl (PC member)
- SIN 2010, Johann Großschadl (PC member)
- WTA 2010, Johann Großschadl (PC member)
- Codebreakers 2010, Peter Ryan (Program chair)
- CeeVote 2010, Peter Ryan (PC member)
- ESORICS 2010, Peter Ryan (PC member)
- WISSEC 2010, Peter Ryan (PC member)
- EVT/WOTE 2010, Peter Ryan (PC member)
- FAST 2010, Peter Ryan (PC member)
- STM 2010, Peter Ryan (PC member)
- PQCrypto 2010, Ralf-Philip Weinmann (PC member)

5.3 Doctoral board

- D. Antonio Lopez Marquez. University of Almeria, December 2010, Prof. Dr. Pascal Bouvry PhD Committee member()
- Remi Sharrock, University of Toulouse, December 2010, Prof. Dr. Pascal Bouvry (PhD Reviewer and Member of the board,)
- Jeremie Albert, University of Bordeaux, December 2010, Prof. Dr. Pascal Bouvry (PhD Reviewer and Member of the board)
- Alfredo Capozuca, University of Luxembourg, December 2010, Prof. Dr. Pascal Bouvry (PhD Chairman of the board)
- Apivadee Piyatumrong, Luxembourg, December 2010, Prof. Dr. Pascal Bouvry (PhD Committee Member)
- Guillermo Molina, University of Malaga, December 2010, Prof. Dr. Pascal Bouvry (PhD Member of the board)
- Tomasz Ignac, University of Luxembourg, July 2010, Prof. Dr. Pascal Bouvry (PhD Chairman of the board)
- Sevil Sen, University of York, June 2010, Prof. Dr. Pascal Bouvry (PhD Reviewer and Member of the board)

- Patrice Caire, University of Luxembourg, March 2010, Prof. Dr. Pascal Bouvry (PhD Chairman of the board)
- Apivadee Piyatumrong, Luxembourg, December 2010, Dr. Grégoire Danoy (PhD Committee Member)
- Nils Bulling, Clausthal University of Technology, Clausthal, Germany, Oct 22 2010, Wojciech Jamroga (PhD committee member)
- Patrice Caire, University of Luxembourg, Luxembourg, Mar 26 2010, Leon van der Torre (Supervisor)
- Chattrakul Sombattheera, The University of Wollongong, Wollongong, Australia, Jul 5 2010, Leon van der Torre (External reviewer)
- Eugen Staab, University of Luxembourg, Luxembourg, Apr 16 2010, Leon van der Torre (Chair)
- Ali Fessi, Munich, Germany, Radu State (Ph.D. Committee Member)
- Maria Biryukov, University of Luxembourg, November 15, 2010, Prof. Dr. Christoph Schommer (Supervisor).
- Sascha Kaufmann (December 10, 2010). Prof. Dr. Christoph Schommer (Supervisor).
- Maria Biryukov; University of Luxembourg; November 15; Prof. Dr. Pierre Kelsen (deputy chairman)
- Sagar Sen; Université de Rennes, Rennes; June 22; Prof. Dr. Pierre Kelsen (rapporteur)
- Barbara Gallina; University of Luxembourg; April 22; Prof. Dr. Pierre Kelsen (jury member)
- Hong-Viet Luong, université Paul Sabatier (Toulouse 3), France, Prof. Dr. Yves Le Traon (Ph.D. Reviewer and Committee Member)
- Fassely DOUMBIA; Institut National Polytechnique de Grenoble en spécialité Mathématique et Informatique, Grenoble (France), Prof. Dr. Yves Le Traon (Ph.D. Reviewer and Committee Member)
- Hakim BELHAOUARI, UPMC, Paris, France, Prof. Dr. Yves Le Traon (Ph.D. Reviewer and Committee Member)
- Freddy Munoz, INRIA Bretagne, Paris, France, Prof. Dr. Yves Le Traon (Ph.D. Committee Member)
- Dmitry Khovratovich, University of Luxembourg, Prof. Dr. Alex Biryukov (PhD Board Member)

- Thomas Icart, University of Luxembourg, Prof. Dr. Alex Biryukov (PhD Board Member)
- Gaetan Leurent ENS, France, Prof. Dr. Alex Biryukov (PhD Board Member)
- Thomas Icart, University of Luxembourg, Prof. Dr. Jean-Sebastien Coron (PhD Board Member)
- Giacomo de Meulenaer, UCL, Belgium, Prof. Dr. Jean-Sebastien Coron (PhD Board Member)
- Georg Fuchsbauer, ENS, France, Prof. Dr. Jean-Sebastien Coron (PhD Board Member)

5.4 Guests

Invited Researchers:

- Prof. Dr. Thomas Agotnes, University of Bergen Norway, Apr 28-29 2010, ICR (Group of Leon van der Torre), talk(s), research collaboration
- Prof. Dr. Guido Boella, University of Torino, Jan-Feb 2010, ICR (Group of Leon van der Torre), AM2c visiting researcher
- Dr. Nils Bulling, Clausthal University of Technology, Germany, Sep 6-10 2010, ICR (Group of Leon van der Torre), talk(s), research collaboration
- Dr. Mehdi Dastani, Utrecht University, The Netherlands, Jun 30 - Jul 7, Sep 6-10 2010, ICR (Group of Leon van der Torre), talk(s), research collaboration
- Dr. Hans van Ditmarsch, University of Sevilla, Spain, Jan 25-29 2010, ICR (Group of Leon van der Torre), talk(s), research collaboration
- Dr. Sujata Ghosh, University of Groningen, Netherlands, Jun 13-16 2010, ICR (Group of Leon van der Torre), talk(s), research collaboration
- Prof. Dr. Valentin Goranko, Technical University of Denmark, Jun 20-25 2010, ICR (Group of Leon van der Torre), talk(s), research collaboration
- Prof. Andreas Herzig, IRIT-CNRS, Mar 7-11 2010, ICR (Group of Leon van der Torre), research collaboration

- Prof. Dr. David Makinson, London School of Economics, LSE, Oct 2010, ICR (Group of Leon van der Torre), talk(s), research collaboration
- Dr. Chattrakul Sombattheera, Mahasarakham University, Thailand, Aug 11 - Oct 15, ICR (Group of Leon van der Torre), AM2c visiting researcher
- Dr. Peter Novak, Czech Technical University, Czech Republic, Nov 29 - Dec 1 2010, ICR (Group of Leon van der Torre), talk(s), research collaboration
- Dr. Ulrich Schäfer, Language Technology Lab, German Research Center for Artificial Intelligence (DFKI), Saarbrücken, Germany. December 2010, Prof. Dr. Christoph Schommer, Talk “Semantic search and visual navigation in scientific publications”
- Prof. Dr. Alain Krief, University Namur, Belgium. October 2010, Prof. Dr. Christoph Schommer, Scientific Exchange regarding a common project.
- Prof. Dr. Marie-Francine Moens, KU Leuven, Belgium, October 2010, Prof. Dr. Christoph Schommer, Talk “Text mining and e-Forensics”.
- Dr. Klaus Julisch, IBM Zurich, Switzerland, November 2010, Prof. Dr. Christoph Schommer, Talk “Optimizing your IT Security Investments”.
- Dr. Merja Heinaniemi, Anke Wienecke, University Luxembourg, November 2010, Prof. Dr. Christoph Schommer, Talk “Data Integration and Mining in Context of Gene Regulation”.
- Prof. Dr. Alfonso Valencia, Spanish Cancer Research Centre, Madrid, Spain, November 2010, Prof. Dr. Christoph Schommer, Talk “Bioinformatics challenges in personalised cancer treatment”
- Prof. Dr. Geoffrey Caruso, University Luxembourg, Luxembourg, November 2010, Prof. Dr. Christoph Schommer, Invited Talk “Data Mining in Geographical Contexts.
- Prof. Dr. Geoffrey Caruso, University Luxembourg, November 2010, Host: Prof. Dr. Christoph Schommer, Talk “Data mining in Geographical Contexts and Texts”.
- Dr. Ivan Laptev, INRIA Paris, France, November 2010, Host: Prof. Dr. Christoph Schommer, Invited Talk “Image and Video Data Mining”.

- Dr. Sabine Erhardt, Federal Office of Criminal Investigation (BKA), Wiesbaden, Germany. December 2010, Prof. Dr. Christoph Schommer, Talk “Forensic Linguistics”.
- Benoit Baudry, INRIA , February 2010, Yves Le Traon

5.5 Visits and other representation activities

- Guillaume Aucher, University of Oxford, Oxford, UK, May 1-8 2010, Research collaboration
- Richard Booth, ISLA 2010 - 3rd Indian School on Logic and its Applications, Hyderabad, India, Jan 25-29 2010, Invited tutorial at the workshop “Alternative approaches to belief change: A consolidated perspective”
- Martin Caminada, Technical University Vienna, Vienna, Austria, Dec 6-8 2010, Presentation at symposium
- Martin Caminada, Sun Yat Sen University, Guangzhou, China, Dec 27 2010, Presentation at symposium
- Wojciech Jamroga, Polish-Japanese School of IT, Gdansk, Poland, Feb 15-16 2010, Research collaboration
- Wojciech Jamroga, University of Amsterdam, Amsterdam, The Netherlands, Mar 8-11 2010, Research collaboration
- Wojciech Jamroga, University of Sevilla, Sevilla, Spain, Mar 29-31 2010, Research collaboration
- Wojciech Jamroga, University of Namur, Namur, Belgium, Apr 20 2010, Research collaboration
- Wojciech Jamroga, Clausthal University of Technology, Clausthal, Germany, May 24-29 2010, Dec 17-23, Research collaboration
- Wojciech Jamroga, Polish Academy of Sciences, Warsaw, Poland, Sep 1-3 2010, Research collaboration
- Marija Slavkovik, University of Turin, Turin, Italy, Mar 21-28 2010, Jun 7-11 2010, Research collaboration with Guido Boella
- Richard Booth, member of the board of the BNVKI (Benelux Association for Artificial Intelligence),
- Emil Weydert, member of the management committee of the COST Action IC0801, Agreement Technologies

- Radu State, University of Zurich, Switzerland, July 07-08 2010 Scientific Cooperation
- Jacques Klein, Fraunhofer, Berlin, Germany, November 17-19 2010, Kickoff European ITEA Project Diamonds
- Jacques Klein, INRIA, Rennes, France, July 11-16 2010, Joint Phd Thesis Supervision
- Yves Le Traon, Jacques Klein, Google, Zurich, Switzerland, June 21-22 2010, Development of Scientific Collaborations
- Yves Le Traon, Jacques Klein, Fraunhofer IESE, Kaiserslautern, Germany, May 26 2010, Development of Scientific Collaborations
- Yves Le Traon, Jacques Klein, KIT, Karlsruhe, Germany, April 29 2010, Development of Scientific Collaborations
- Yves Le Traon, Jacques Klein, Saarland University, Saarbrücken, Germany, July 5 2010, Development of Scientific Collaborations
- Yves Le Traon, Telecom Bretagne, Rennes, France, several meetings in the year 2010 for continuous collaboration
- Yves Le Traon, INRIA Bretagne Atlantique, Triskell team, Rennes, France, several meetings in the year 2010, for continuous research collaboration Kickoff European ITEA Project Diamonds
- Peter Ryan, [CRP Workshop on Security and Trust](#), 10-11 January 2010, Invited Talk
- Peter Ryan, [Polish/Luxembourg Workshop on Security and Trust](#), 6-7 May 2010, Invited Talk
- Peter Ryan, [Dagstuhl Workshop on Insider Threats](#), 22-26 August 2010, Invited Talk
- Peter Ryan, [Swiss e-voting Workshop](#), 6 September and joint Workshop with NIST, 7th September, Invited Talk
- Peter Ryan, [Jean-Jaques Quisquater Emeritus day](#), 26 November, Invited Talk
- Peter Ryan, [Invited talk at IMT Lucca](#), 18 November, Invited Talk
- Peter Ryan, [Invited Talk at the Cryptoforma Workshop](#), 22 October, Invited Talk

5.6 Research meeting

5.6.1 ILIAS

ILIAS: ILIAS Seminar, Wednesdays 4pm, 13 presentations

Optimization and Parallel Computing : Eight research team meetings and one yearly team meeting with 15 presentations organized in October. All schedules and sources available at <http://teambouvry.gforge.uni.lu>. Two Working Group meetings with invited speakers, schedules available [here](#)

ICR: typically weekly (Monday 16pm); Seminar with guest researchers/Internal seminar.

MINE: Research Seminars are quarterly events, which aim at the transfer of knowledge inside the group, but also focus on transparency and visibility in general. The seminars are organised on a daily basis and include demonstrations and presentations, discussions and evaluations.

5.6.2 LASSY

[LASSY Seminars](#), 6 presentations

5.6.3 SaToSS Research Meeting

Every Tuesday from 10:30 to 11:30 the members of the Security and Trust of Software Systems group (SaToSS) have the SaToSS Research Meeting (SRM). Saša Radomirović is responsible for the organization of the SRM. The meeting featured 27 presentations in 2010. The complete list of speakers can be found [here](#).

CSC Software

6.1 GreenCloud

- <https://gforge.uni.lu/projects/greencloud/>
- Energy efficiency simulator for distributed data centers .

6.2 OVINS

- <http://ovnis.gforge.uni.lu/>
- For online vehicular wireless and traffic simulation. An integration of traffic simulator SUMO with network simulator ns-3.

6.3 VehILux

- <https://github.com/pigne/VehILux>
- A realistic vehicular mobility model for Luxembourg based on real traffic data.

6.4 SHARC

- Licence: GPL v3
- <http://github.com/gjherbiet/sharc>
- Description: Source code and benchmarking framework for the SHARC (Sharper Heuristic for Assignment of Robust Communities) protocol

6.5 An Implementation of Basic Argumentation Components - ArguLab 0.2

- Developers: Mikolaj Podlaszewski, Yining Wu, Martin Caminada
- Licence: GPL v3.0
- <http://heen.webfactional.com/>
- With this demonstrator we present an implementation of formal argumentation that exploits some results of formal argumentation theory. The current demonstrator can generate not only grounded, preferred, stable, and semi-stable extensions, but also stage labelings. The software is able to defend its answer by entering a discussion game with the user.

6.6 Adaptive High-Interaction Honeypot Alternative (AHA)

- Licence: GPL
- Weblink: <http://git.quuxlabs.com/?p=aha-linux-2.6/.git;a=summary>
- Description: AHA is an implementation of a high-interaction honeypot in order to optimize information retrieval from attackers, including measurements of their skills and their ethnic background. It is a modified User-Mode-Linux with an additional python decision making framework for implementing intelligent honeypots.

6.7 MiCS Management System

- Licence: non-redistributable, for internal use only.

- <http://demos.uni.lux/mics>
- An internal web-based tool developed for the management of modules, courses and profiles of the Master in Information and Computer Sciences. Developed by Christian Glodt.

6.8 bagit

- Licence: non-redistributable, for internal use only.
- <http://demos.uni.lux/bagit>
- An internal web-based tool that provides assistance to research groups by storing, pooling, tagging and indexing papers and other publications. Developed by Christian Glodt.

6.9 Visual Contract Builder

- Licence: free to use, binary redistribution permitted.
- <http://vcl.gforge.uni.lu>
- Eclipse plugins that provide support for graphically editing and type-checking VCL (Visual Contract Language) diagrams. Developed by Christian Glodt and Nuno Amalio.

6.10 Model Decomposer

- Licence: free to use, binary redistribution permitted.
- <http://democles.lassy.uni.lu>, http://democles.lassy.uni.lu/documentation/TR_LASSY_10_06.pdf
- An Eclipse plugin that implements a generic model decomposition technique which is applicable to Ecore instances and EP models, and is described in a paper accepted for publication in the proceedings of the FASE 2011 conference. Developed by Christian Glodt.

CSC Publications in 2010

The publications listed in this chapter have been generated from the official publication record repository of the university:

<http://publications.uni.lu>

An overview of the publication quantity (per category) is provided in the table below.

Publication category	Quantity	Section
Books	4	§7.1 page 121
Book Chapters	13	§7.2 page 122
Book Chapters	1	§7.3 page 124
International journals	41	§7.4 page 124
Conferences Articles	184	§7.5 page 127
PhD Thesis	5	§7.6 page 146
Internal Reports	8	§7.7 page 146
Proceedings	5	§7.8 page 147
Total:	261	

Table 7.1: Overview of CSC publications in 2010

7.1 Books

- [1] Jianguo Ding. *Advances in Network Management*. CRC press, Taylor & Francis Group, USA, 2010.

- [2] Wisam Al Abed, Nuno Amálio, Vasco Amaral, Olivier Barais, Bruno Barroca, Benoît Baudry, Emmanuel Bertin, Nicolas Bertrand, Nicolas Boizot, Erwan Brottier, Eric Busvelle, E. C. de Almeida, Alfredo Capozucca, Sergio Coronado, Stephen Creff, Romain Delamare, Philippe Dhaussy, J. E. Marynowski, Marwane El Kharbili, Roberto Felix, Franck Fleurey, Robert France, Barbara Gallina, Jean-Paul Gauthier, Sudipto Ghosh, Christian Glodt, Nicolas Guelfi, Hristomir Hristov, Jean-Marc Jezequel, Pierre Kelsen, Jorg Kienzle, Jacques Klein, Yves Le Traon, Yiqing Li, Levi Lucio, J. M. Mottu, Qin Ma, Brice Morin, Tejeddine Mouelhi, Freddy Munoz, Simin Nadjm-Tehrani, Gilles Perrouin, Pierre-Yves Pillain, Cedric Pruski, Amine Raji, Chantal Reynaud, Andreas Rusnjak, Jurgen Sachau, Ayda Saidane, Gabriel Sandulescu, Peter Schaffer, Kenneth Sebesta, Sagar Sen, Jacques Simonin, Vasco Sousa, Andreas Speck, G. Sunye, Eric Totel, P. Valduriez, Valerie Viet Triem Tong, Federico Wiecko, and Denis Zampunieris. *LASSY - Laboratory for Advanced Software Systems - Scientific Publications List 2010*. Imprimerie Klopp, 2010.
- [3] Guido Boella, Gabriella Pigozzi, Munindar P. Singh, and Harko Verhagen. *Normative Multiagent Systems: Guest Editors' Introduction*, volume 18. 2010.
- [4] D. M. Gabbay, M. Abraham, and U. Schild. *Non-Deductive Inference in the Talmud*. 2010.

7.2 Book Chapters

- [5] Xavier Parent and Leendert van der Torre. Input/output logics. In *9th De Morgan Workshop on Deontic Logic*. 2009.
- [6] Guillaume Aucher. Characterizing updates in dynamic epistemic logic. In *Knowledge Representation and Reasoning (KR 2010)*, pages 135–142. 2010.
- [7] Guillaume Aucher, Guid Boella, and Leon van der Torre. Prescriptive and descriptive obligations in dynamic epistemic deontic logic. In *AICOL Workshop (2009)*, pages 150–161. 2009.
- [8] Thomas Schaberreiter, Cédric Bonhomme, Jocelyn Aubert, Christophe Incoul, and Djamel Khadraoui. Support tool development for real-time risk prediction in interdependent critical infrastructures. In *IEEE International Symposium on Software Reliability Engineering (ISSRE) supplemental proceedings*, pages 00–00. 2009.

- [9] Jocelyn Aubert, Thomas Schaberreiter, Christophe Incou, and Djamel Khadraoui. Real-time security monitoring of interdependent services in critical infrastructures. case study of a risk-based approach. In *in 21th European Safety and Reliability Conference (ESREL 2010)*, pages 00–00. 2009.
- [10] Jocelyn Aubert, Thomas Schaberreiter, Christophe Incou, Djamel Khadraoui, and Benjamin Gateau. Risk-based methodology for real-time security monitoring of interdependent services in critical infrastructures. In *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, pages 262–267. 2010.
- [11] Cynthia Wagner, Gerard Wagener, Radu State, and Thomas Engel. Malware analysis with graph kernels and support vector machines. In *4th International Conference on Malicious and Unwanted Software (Malware 2009)*, pages 63–68. IEEE, 2009.
- [12] Cynthia Wagner, Gerard Wagener, Radu State, Alexandre Dulaunoy, and Thomas Engel. Game theory driven monitoring of spatial-aggregated ip flow records. In *Proceedings of the 6th International Conference on Network and Services Management (CNSM)*, pages 0–0. IEEE, 2010.
- [13] Jérôme François, Humberto Abdelnur, Radu State, and Olivier Festor. Semi-supervised fingerprinting of protocol messages. In *Proceedings of the 3rd International Conference on Computational Intelligence in Security for Information Systems*, volume 85, pages 107–115. Springer, 2010.
- [14] Jérôme François, Radu State, Thomas Engel, and Olivier Festor. Digital forensics in voip networks. In *Workshop on Information Forensics and Security*, pages 0–0. IEEE, 2010.
- [15] David Fotue, Foued Melakessou, Thomas Engel, and Houda Labiod. Design of new aggregation techniques for wireless sensor networks. In *The 18th Annual Meeting of the IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, pages 1–1. MASCOTS, 2010.
- [16] D. Dunlop, S. Varrette, and Pascal Bouvry. Deskillig hpl - using an evolutionary algorithm to automate cluster benchmarking. In *Proc. of 8th Intl. conf. on Parallel Processing and Applied Mathematics (PPAM 2009)*, LNCS. Springer Verlag, 2010.
- [17] Nicolas Boizot, Eric Busvelle, and Jean-Paul Gauthier. Adaptive-gain extended kalman filter: Extension to the continuous-discrete case.

In *In Proceeding of the 10th European Control Conference (ECC'09)*. 2009.

7.3 Book Chapters

- [18] David Galindo and Eric R. Verheul. *Pseudonymized Data Sharing*, volume 3 of *Advanced Information and Knowledge Processing*, pages 157–179. Springer, 2010.

7.4 International journals

- [19] Xavier Parent. A complete axiom set for hansson’s deontic logic dsdl2. *Logic Journal of the IGPL*, 18(3):422–429, 2010.
- [20] Gérard Wagener, Radu State, Alexandre Dulaunoy, and Thomas Engel. Heliza: talking dirty to the attackers. *Journal in Computer Virology*, pages 1–12, 2010. 10.1007/s11416-010-0150-4.
- [21] Jérôme François, Humberto Abdelnur, Radu State, and Olivier Festor. Machine learning techniques for passive network inventory. *Transactions on Network and Service Management*, 7(4):244 – 257, 2010.
- [22] Thomas Scherer Raphael Frank and Mario Gerla. Edfs a novel flooding protocol for multi-hop wireless networks. pages 349–354, February 2010.
- [23] Giovanni Pau Eugenio Giordano, Raphael Frank and Mario Gerla. Corner: a realistic urban propagation model for vanet. pages 99–105, February 2010.
- [24] Giovanni Pau Eugenio Giordano, Raphael Frank and Mario Gerla. Corner: A step towards realistic simulations for vanet. pages 41–50, September 2010.
- [25] Pasquale Cataldi Raphael Frank, Eugenio Giordano and Mario Gerla. Trafroute: An different approach to routing in vehicular networks. pages 521–528, October 2010.
- [26] Benjamin Braatz, Ulrike Golas, and Thomas Soboll. How to delete categorically. two pushout complement constructions. *Journal of Symbolic Computation*, pages 1–32, 2010. Accepted for Publication.
- [27] G. Pigozzi. Belief merging and the discursive dilemma: an argument-based account to paradoxes of judgment aggregation. *Synthese*, 152(2):285–298, 2006.

- [28] Marek Ostaszewski, Franciszek Seredynski, and Pascal Bouvry. Coevolutionary-based mechanisms for network anomaly detection. *Journal of Mathematical Modelling and Algorithms*, 6(3):411 – 431, 2007.
- [29] Hugo Jonker, Melanie Volkamer, A. Alkassar, and M. Volkamer. Compliance of rics to the proposed e-voting protection profile. *Lecture Notes in Computer Science*, 4896:50–61, 2007.
- [30] F. Khafa, E. Alba, B. Dorransoro, and B. Duran. Efficient batch job scheduling in grids using cellular genetic algorithms. *Journal Of Mathematical Modelling and Algorithms*, 7(2):217 – 236, 2008.
- [31] Le Hoai Minh, Le Thi Hoai An, Pham Dinh Tao, and Pascal Bouvry. A combined dca: Ga for constructing highly nonlinear balanced boolean functions in cryptography. *J. Global Optimization*, 47(4):597–613, 2010.
- [32] Alex Biryukov and Adi Shamir. Structural cryptanalysis of sasas. *Journal of Cryptology*, 23(4):505–518, 2010.
- [33] Erkki Lehtonen. A note on minors determined by clones of semilattices. *Novi Sad Journal of Mathematics*, 40(3):75–81, 2010.
- [34] Stephan Hartmann, Gabriella Pigozzi, and Jan Sprenger. Reliable methods of judgement aggregation. *J. Log. Comput.*, 20(2):603–617, 2010.
- [35] Patrice Caire and Leendert van der Torre. Convivial ambient technologies: Requirements, ontology and design. *Comput. J.*, 53(8):1229–1256, 2010.
- [36] Dov M. Gabbay and Karl Schlechta. A theory of hierarchical consequence and conditionals. *Journal of Logic, Language and Information*, 19(1):3–32, 2010.
- [37] Dov M. Gabbay and Karl Schlechta. A comment on work by booth and co-authors. *Studia Logica*, 94(3):403–432, 2010.
- [38] Richard Booth and Thomas Meyer. Equilibria in social belief removal. *Synthese*, 177, 2010.
- [39] Y. Wu and M.W.A. Caminada. A labelling-based justification status of arguments. *Studies in Logic*, 3:12–29, 2010.
- [40] Antonis Bikakis and Grigoris Antoniou. Defeasible contextual reasoning with arguments in ambient intelligence. *IEEE Transactions on Knowledge and Data Engineering*, 22(11):1492–1506, 2010.

- [41] I. Seylan and W. Jamroga. Coalition description logic for individuals. *Electronic Notes in Theoretical Computer Science*, 262:231–248, 2010.
- [42] R. van der Meyden and Chenyi Zhang. A comparison of semantic models for noninterference. *Theoretical Computer Science*, 411:4123–4147, 2010.
- [43] N. Bulling and W. Jamroga. Verifying agents with memory is harder than it seemed. *AI Communications*, 23:380–403, 2010.
- [44] Gerard Wagener, Radu State, Alexandre Dulaunoy, and Thomas Engel. Heliza: talking dirty to the attackers. *Journal in Computer Virology*, pages 1–12, 2010.
- [45] Grégoire Danoy, Pascal Bouvry, and Olivier Boissier. A multi-agent organizational framework for coevolutionary optimization. *LNCS Transactions on Petri Nets and Other Models of Concurrency IV*, 4:199–224, 2010.
- [46] Ingo Scholtes, Jean Botev, Markus Esch, and Peter Sturm. Epidemic self-synchronization in complex networks of kuramoto oscillators. *Advances in Complex Systems (ACS)*, 13(1):33 – 58, 2010.
- [47] Jean Botev, Markus Esch, Hermann Schloss, Ingo Scholtes, and Peter Sturm. Hyperverse: Simulation and testbed reconciled. *International Journal of Advanced Media and Communication (IJAMC)*, 4(2):167 – 181, 2010.
- [48] Zdzislaw Suchanecki and Fernando Gomez-Cubillo. Evolution semi-groups and time operators on banach spaces. *Journal of Mathematical Analysis and Applications*, 371(2):454–464, 2010.
- [49] Nuno Amalio, Pierre Kelsen, Qin Ma, and Christian Glodt. Using vcl as an aspect-oriented approach to requirements modelling. *Transactions on Aspect Oriented Software Development*, 7:151–199, 2010.
- [50] Stephan Foldes and Erkkö Lehtonen. Column-partitioned matrices over rings without invertible transversal submatrices. *Ars Combinatoria*, 97:33–39, 2010.
- [51] Pascal Schweitzer and Patrick Schweitzer. Connecting face hitting sets in planar graphs. *Information Processing Letters*, 111(1):11–15, 2010.
- [52] Erkkö Lehtonen. Closed classes of functions, generalized constraints and clusters. *Algebra Universalis*, 63(2-3):203–234, 2010.
- [53] Erkkö Lehtonen. Characterization of preclones by matrix collections. *Asian-European Journal of Mathematics*, 3(3):457–473, 2010.

- [54] Nicolas Boizot, Eric Busvelle, and Jean-Paul Gauthier. An adaptive high-gain observer for nonlinear systems. *Automatica (Journal of IFAC)*, 46(9):1483–1488, 2010.
- [55] Erkkko Lehtonen and Agnes Szendrei. The submaximal clones on the three-element set with finitely many relative r-classes. *Discussiones Mathematicae - General Algebra and Applications*, 30(1):7–33, 2010.
- [56] Erkkko Lehtonen and Jaroslav Nešetřil. Minors of boolean functions with respect to clique functions and hypergraph homomorphisms. *European Journal of Combinatorics*, 31(8):1981–1995, 2010.
- [57] Frank C. Krysiak and Patrick Schweitzer. The optimal size of a permit market. *Journal of Environmental Economics and Management*, 60(2):133–143, 2010.
- [58] Gabriel Sandulescu and Simin Nadjm-Tehrani. Adding redundancy to replication in window-aware delay-tolerant routing. *Journal of Communications*, 5(2):117–129, 2010.
- [59] Alfredo Capozucca and Nicolas Guelfi. Modelling dependable collaborative time-constrained business process. *Enterprise Information System*, 4(2):153–214, 2010.

7.5 Conferences Articles

- [60] Guillaume Aucher, Davide Grossi, Andreas Herzig, and Emiliano Lorini. Dynamic context logic. In X. (Editor) He, J. (Editor) Horty, and E. (Editor) Pacuit, editors, *Proceedings of Logic, Rationality and Interaction (LORI 2009)*, volume 5884. 5884 of *Lecture Notes in Artificial Intelligence*, pages 15–26. Springer Verlag, 2009.
- [61] Guillaume Aucher. Bms revisited. In *Theoretical Aspects of Rationality and Knowledge (TARK 2009)*, pages 24–33, 2009.
- [62] Davide Grossi, Gabriella Pigozzi, and Marija Slavkovic. White manipulation in judgment aggregation. In *Proceedings of BNAIC 2009 - The 21st Benelux Conference on Artificial Intelligence (to appear)*, 2009.
- [63] Gabriella Pigozzi, Marija Slavkovic, and Leendert van der Torre. A complete conclusion-based procedure for judgment aggregation. In *Proceedings of the First International Conference on Algorithmic Decision Theory (ADT)*, volume 5783. 5783 of *Lecture Notes in Artificial Intelligence*, pages 1–13. Springer Verlag, 2009.

- [64] I. Seylan and W. Jamroga. Description logic for coalitions. In *Proceedings of AAMAS'09*, pages 425–432, 2009.
- [65] I. Seylan and W. Jamroga. Coalition description logic for individuals. In *Proceedings of the 6th Workshop on Methods for Modalities M4M-6*, pages 146–162, 2009.
- [66] Guillaume Aucher, Guido Boella, and Leendert van der Torre. Prescriptive and descriptive obligations in dynamic epistemic deontic logic. In *AICOL Workshops*, pages 150–161, 2009.
- [67] Guido Boella, Guido Governatori, Antonino Rotolo, and Leendert van der Torre. *ex Minus Dixit Quam Voluit, ex magisdixit quam voluit*: A formal study on legal compliance and interpretation. In *AICOL Workshops*, pages 162–183, 2009.
- [68] Guido Boella, Souhila Kaci, and Leendert van der Torre. Dynamics in argumentation with single extensions: attack refinement and the grounded extension. In *AAMAS (2)*, pages 1213–1214, 2009.
- [69] Guido Boella, Leendert van der Torre, and Serena Villata. Conditional dependence networks in requirements engineering. In *COIN@AAMAS&IJCAI&MALLOW*, pages 3–18, 2009.
- [70] Julien Schleich, Grégoire Danoy, Pascal Bouvry, and An Le Thi Hoai. Backbone2, an efficient deterministic algorithm for creating 2-connected m-dominating set-based backbones in ad hoc networks. In *Proceedings of the Seventh ACM International Workshop on Mobility Management & Wireless Access*, pages 91–98, 2009.
- [71] Julien Schleich, Pascal Bouvry, and An Le Thi Hoai. Decentralized fault-tolerant connected dominating set algorithm for mobile ad hoc networks. In *Proceedings of the 2009 International Conference on Wireless Networks*, pages 354–360, 2009.
- [72] Michael Stieghahn and Thomas Engel. Law-aware access control for international financial environments. In *MobiDE '09: Proceedings of the Eighth ACM International Workshop on Data Engineering for Wireless and Mobile Access*, pages 33–40. ACM New York, NY, USA, 2009.
- [73] Michael Stieghahn and Thomas Engel. Using xacml for law-aware access control. In *3rd. International Workshop on Juris-informatics (JURISIN 2009)*, 2009.
- [74] Barbara Kordy, Sjouke Mauw, Saša Radomirović, and Patrick Schweitzer. Foundations of attack–defense trees. In Joshua Guttman

- Pierpaolo Degano, Sandro Etalle, editor, *Proceedings of the 7th international Workshop on Formal Aspects in Security and Trust (FAST 2010)*, volume 6561 of *LNCS*. Springer, 2011. To appear.
- [75] Pierre Kelsen and Qin Ma. A lightweight approach for defining the formal semantics of a modeling language. In *ACM/IEEE 11th International Conference on Model Driven Engineering Languages and Systems (MODELS 2008)*, volume 5301. 5301 of *Lecture Notes in Computer Science*, pages 5301 – 690. Springer Berlin / Heidelberg, 2008.
- [76] Marek Ostaszewski, Pascal Bouvry, and Franciszek Seredynski. Adaptive and dynamic intrusion detection by means of idiotypic networks paradigm. In *The 21th IEEE International Parallel and Distributed Processing Symposium (IPDPS), NIDISC Workshop.*, pages 1 – 8. IEEE Computer Society, 2008.
- [77] Marek Ostaszewski, Pascal Bouvry, and Franciszek Seredynski. An approach to intrusion detection by means of idiotypic networks paradigm. In *IEEE World Congress on Computational Intelligence, WCCI 2008, Congress on Evolutionary Computation CEC 2008, Honk-Kong, June*. IEEE Computer Society, 2008.
- [78] Marek Ostaszewski, Pascal Bouvry, and Franciszek Seredynski. Denial of service detection and analysis using idiotypic networks paradigm. In *Proceedings of Genetic and Evolutionary Computation Conference (GECCO 2008)*, pages 79 – 86. ACM, 2008.
- [79] F. Khafa, J. Carretero, B. Dorronsoro, and E. Alba. Design and evaluation of a tabu search method for job scheduling in distributed environments. In *The 21th IEEE International Parallel and Distributed Processing Symposium (IPDPS), NIDISC Workshop.*, page 11. IEEE Computer Society, 2008.
- [80] Sebastien Varrette, Marek Ostaszewski, and Pascal Bouvry. Nature inspired algorithm-based fault tolerance on global computing platforms. application to symbolic regression. In *International Conference on Metaheuristics and Nature Inspired Computing (META'08)*, 2008.
- [81] Ton van Deursen and Sasa Radomirović. Security of an rfid protocol for supply chains. In *Proceedings of the 1st Workshop on Advances in RFID, AIR'08*, pages 568 – 573. IEEE Computer Society, 2008.
- [82] Jean-Sébastien Coron, Jacques Patarin, and Yannick Seurin. The random oracle model and the ideal cipher model are equivalent. In *CRYPTO*, pages 1 – 20, 2008.

- [83] Apivadee Piyatumrong, Pascal Bouvry, Frederic Guinand, and Kit-tichai Lavangnananda. Trusted spanning tree for delay tolerant manets. In *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008, EUC'08*, volume 2, pages 293 – 299, 2008.
- [84] Apivadee Piyatumrong, Pascal Bouvry, Frederic Guinand, and Kit-tichai Lavangnananda. Trusted spanning trees for delay tolerant mobile ad hoc networks. In *IEEE Conference on Soft Computing in Industrial Applications, 2008. SMCia '08*, pages 131 – 136, 2008.
- [85] Aida Vosoughi, Kashif Bilal, Samee Ullah Khan, Nasro Min-Allah, Juan Li, Nasir Ghani, Pascal Bouvry, and Sajjad Madani. A multidimensional robust greedy algorithm for resource path finding in large-scale distributed networks. In *Proceedings of the 8th International Conference on Frontiers of Information Technology (FIT'2010)*, volume 4, pages 1–6. ACM, 2010.
- [86] Siqian Liu, Kashif Bilal, Samee Ullah Khan, Hongxiang Li, Nasro Min-Allah, Juan Li, Nasir Ghani, Pascal Bouvry, and Sajjad Madani. Heuristics-based nominal channels allocation in cellular networks. In *Proceedings of the 8th International Conference on Frontiers of Information Technology (FIT'2010)*, pages 1–4. ACM, 2010.
- [87] Ranganai Chaparadza, Symeon Papavassiliou, Said Souli, and Jianguo Ding. The self-managing future internet powered by the current ipv6 and extensions to ipv6 towards "ipv6++"—a viable roadmap scenario for the internet evolution path. In *Proceedings of the IEEE Globecom 2010 Workshop on Management of Emerging Networks and Services*, pages 551–556. IEEE communication society press, 2010.
- [88] Nuno Amalio and Pierre Kelsen. Visual behavioral modelling with contracts. In *FLACOS 2010*, pages 0–0, 2010.
- [89] Sergio Coronado and Denis Zampunieris. Continuous proactivity in learning management systems. In *EDUCON 2010 - The Future of Global Learning in Engineering Education*, volume 1, pages 1–201. IEEE, 2010.
- [90] Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir. Key recovery attacks of practical complexity on aes-256 variants with up to 10 rounds. In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lecture Notes in Computer Science*, volume 6110, pages 299–319. Springer, 2010.

- [91] Rishiraj Bhattacharyya, Avradip Mandal, and Mridul Nandi. Security analysis of the mode of jh hash function. In *Fast Software Encryption, 17th International Workshop, FSE 2010, Seoul, Korea, February 7-10, 2010*, volume 6147, pages 168–191. LNCS, Springer, 2010.
- [92] Emilia Tantar. A priori landscape analysis in bi-objective combinatorial optimization. In *Proceedings of The 6th European Conference on Intelligent Systems and Technologies*, pages 1–7, 2010.
- [93] Johnatan E. Pecero, Pascal Bouvry, and Carlos J. Barrios. Low energy and high performance scheduling on scalable computing systems. In *Latin-American Conference on High Performance Computing*, pages 1–8, 2010.
- [94] Guillaume-Jean HERBIET and Pascal BOUVRY. Sharc: Community-based partitioning for mobile ad hoc networks using neighborhood similarity. In *World of Wireless Mobile and Multimedia Networks (WoW-MoM), 2010 IEEE International Symposium on a*, pages 1 – 9, 2010.
- [95] Jean-Francois Gallais, Johann Grouschadl, Neil Hanley, Markus Kasper, Marcel Medwed, Francesco Regazzoni, Jorn-Marc Schmidt, Stefan Tillich, and Marcin Wojcik. Hardware trojans for inducing or amplifying side-channel leakage of cryptographic software. In *Second International Conference on Trusted Systems (INTRUST 2010)*, pages 00–00, Beijing, China, December 2010. Springer Verlag.
- [96] Johann Grosschadl and Ilya Kizhvatov. Performance and security aspects of client-side ssl/tls processing on mobile devices. In *Cryptology and Network Security — CANS 2010*, volume LNCS 6467, pages 44–61. Springer Verlag, 2010.
- [97] Zhe Liu, Johann Grosschadl, and Ilya Kizhvatov. Efficient and side-channel resistant rsa implementation for 8-bit avr microcontrollers. In *Proceedings of the 1st Workshop on the Security of the Internet of Things (SECIOT 2010)*, pages 00–00. IEEE Computer Society, 2010.
- [98] Johann Grosschadl, Matthias Hudler, Manuel Koschuch, Michael Kruger, and Alexander Szekely. Smart elliptic curve cryptography for smart dust. In *Quality of Service in Heterogeneous Networks — QSHINE 2010*, pages 00–00. Springer Verlag, 2010.
- [99] Marcel Medwed, Francois-Xavier Standaert, Johann Grosschadl, and Francesco Regazzoni. Fresh re-keying: Security against side-channel and fault attacks for low-cost devices. In *Progress in Cryptology — AFRICACRYPT 2010*, volume LNCS 6055, pages 279–296. Springer Verlag, 2010.

- [100] Jean-Francois Gallais, Ilya Kizhvatov, and Michael Tunstall. Improved trace-driven cache-collision attacks against embedded aes implementations. In *Proceedings of the 11th international conference on Information security applications (WISA 2010)*, pages 243–257, Jeju Island, Korea, 2010. Springer-Verlag.
- [101] Martin Caminada and Mikolaj Podlaszewski. An implementation of basic argumentation components. In *Proceedings of the DEMO session of the Third International Conference on Computational Models of Argument (COMMA) (2010)*, pages 0–0, 2010.
- [102] Martin Caminada, Gabriella Pigozzi, and Mikolaj Podlaszewski. Manipulation in group argument evaluation. In *Proceedings of the eleventh AI*IA symposium on artificial intelligence (2010)*, pages 209–216, 2010.
- [103] Zhe Xia, Chris Culnane, James Heather, Hugo Jonker, Peter Ryan, Steve Schneider, and Sriramkrishnan Srinivasan. Versatile pret a voter: Handling multiple election methods with a unified interface. In *Proceedings of the 11th International Conference on Cryptology in India (Indocrypt'10)*, pages 98–114, 2010.
- [104] Malika Mehdi, Nouredine Melab, El-Ghazali Talbi, and Pascal Bouvry. Interval-based initialization method for permutation-based problems. In *IEEE Congress on Evolutionary Computation (CEC), 2010*, pages 1–8. IEEE, 2010.
- [105] Karsten Nohl, Erik Tews, and Ralf-Philipp Weinmann. Cryptanalysis of the dect standard cipher. In *Lecture Notes in Computer Science*, volume 6147, pages 1–18. Springer, 2010.
- [106] Peter Ryan, James Heather, and Vanessa Teague. Pretty good democracy for more expressive voting schemes. In *Computer Security – ESORICS 2010 15th European Symposium on Research in Computer Security, Athens, Greece, September 20-22, 2010. Proceedings*, pages 405 – 423, 2010.
- [107] Alex Biryukov, Deike Priemuth-Schmid, and Bin Zhang. Multiset collision attacks on reduced-round snow 3g and snow 3g (+). In *Lecture Notes in Computer Science*, volume 6123, pages 139–153. Springer-Verlag, 2010.
- [108] Dmitry Khovratovich, Ivica Nikolic, and Christian Rechberger. Rotational rebound attacks on reduced skein. In *ASIACRYPT*, pages 1–19, 2010.

- [109] Alex Biryukov and Ivica Nikolic. Automatic search for related-key differential characteristics in byte-oriented block ciphers: Application to aes, camellia, khazad and others. In *EUROCRYPT*, pages 322–344, 2010.
- [110] Dmitry Khovratovich and Ivica Nikolic. Rotational cryptanalysis of arx. In *Fast Software Encryption*, pages 333–346, 2010.
- [111] David Galindo, Benoît Libert, Marc Fischlin, Georg Fuchsbauer, Anja Lehmann, Mark Manulis, and Dominique Schroder. Public-key encryption with non-interactive opening: New constructions and stronger definitions. In *Progress in Cryptology - AFRICACRYPT 2010, Third International Conference on Cryptology in Africa*, volume 6055, pages 333–350. Springer, 2010.
- [112] David Galindo. Chosen-ciphertext secure identity-based encryption from computational bilinear diffie-hellman. In *Pairing-Based Cryptography - Pairing 2010 - 4th International Conference*, volume 6487, pages 367–376. Springer Verlag, 2010.
- [113] Benjamin Braatz and Christoph Brandt. How to modify on the semantic web? In *Current Trends in Web Engineering*, volume 6385, pages 187–198. Springer Lecture Notes in Computer Science, 2010.
- [114] Benjamin Braatz, Hartmut Ehrig, Karsten Gabriel, and Ulrike Golas. Finitary m-adhesive categories. In *Graph Transformations*, volume 6372, pages 234–249. Springer Lecture Notes in Computer Science, 2010.
- [115] Farah Benamara, Souhila Kaci, and Gabriella Pigozzi. Individual opinions-based judgment aggregation procedures. In *MDAI*, pages 55–66, 2010.
- [116] Martin Caminada, Gabriella Pigozzi, and Mikolaj Podlaskowski. Manipulation in group argument evaluation. In *Procs. of the 8th European Workshop on Multi-agent Systems (EUMAS'10)*, 2010.
- [117] Yining Wu. Transforming fuzzy description logic alc-fl into classical description logic alch. In *Proceedings of the 6th International Workshop on Uncertainty Reasoning for the Semantic Web (URSW 2010)*, 2010.
- [118] Guido Boella, Guido Governatori, Antonino Rotolo, and Leendert van der Torre. A logical understanding of legal interpretation. In *KR*, 2010.
- [119] Guido Boella, Dov M. Gabbay, Valerio Genovese, and Leendert van der Torre. Higher-order coalition logic. In *ECAI*, pages 555–560, 2010.

- [120] Guillaume Aucher, Guido Boella, and Leendert van der Torre. Privacy policies with modal logic: The dynamic turn. In *DEON*, pages 196–213, 2010.
- [121] Leendert van der Torre. Deontic redundancy: A fundamental challenge for deontic logic. In *DEON*, pages 11–32, 2010.
- [122] Guido Boella, Dov M. Gabbay, Leendert van der Torre, and Serena Villata. Support in abstract argumentation. In *Proceedings of the Third International Conference on Computational Models of Argument (COMMA'10)*, pages 40–51. Frontiers in Artificial Intelligence and Applications, IOS Press, 2010.
- [123] Serena Villata, Guido Boella, Dov M. Gabbay, and Leendert van der Torre. Arguing about trust in multiagent systems. In *Proceedings of the 11th Symposium on Artificial Intelligence of the Italian Association for Artificial Intelligence (AIIA'10)*, pages 236–243, 2010.
- [124] Guido Boella, Leendert van der Torre, and Serena Villata. Trust in abstract argumentation. In *Proceedings of the 4th Mahasarakham International Workshop on Artificial Intelligence (MIWAI'10)*, 2010.
- [125] Guido Boella, Gabriella Pigozzi, Marija Slavkovic, and Leendert van der Torre. Group intentions are social choice with commitment. In *Procs. of the 8th European Workshop on Multi-agent Systems (EU-MAS'10)*, 2010.
- [126] Guido Boella, Gabriella Pigozzi, Marija Slavkovic, and Leendert van der Torre. Group intentions are social choice with commitment. In *Pre-Procs. of the 11th International Workshop on Coordination, Optimization, Institution and Norms in Multiagent Systems (COIN@MALLOW'10)*, pages 115–133, 2010.
- [127] Matteo Baldoni, Guido Boella, Valerio Genovese, Andrea Mugnaini, Roberto Grenna, and Leendert van der Torre. A middleware for modelling organizations and roles in jade. In *Post-proceedings of the 7th International Workshop on Programming Multi-Agent Systems (Promas 2009)*, 2010.
- [128] Guido Boella, Dov M. Gabbay, Alan Perotti, and Serena Villata. Coalition formation via negotiation in multiagent systems with voluntary attacks. In *Procs. of the 22th Belgian-Netherlands Conference on Artificial Intelligence (BNAIC'10)*, pages 25–32, 2010.
- [129] Guido Boella, Dov M. Gabbay, and Serena Villata. Subsumption and count as relation in arguments ontologies. In *Procs. of the 13th International Workshop on Non-Monotonic Reasoning (NMR'10)*, 2010.

- [130] Xavier Parent. Moral particularism and deontic logic. In *DEON*, pages 84–97, 2010.
- [131] Michael Abraham, Dov M. Gabbay, and Uri J. Schild. Obligations and prohibitions in talmudic deontic logic. In *DEON*, pages 166–178, 2010.
- [132] V. Genovese, D. Rispoli, L. van der Torre, and D. M. Gabbay. Modal access control logic. pages 114–126, 2010.
- [133] Valerio Genovese, Laura Giordano, Valentina Gliozzi, and Gian Luca Pozzato. A constructive conditional logic for access control: a preliminary report. In *ECAI*, pages 1073–1074, 2010.
- [134] Steve Barker and Valerio Genovese. A logic of privacy. In *DBSec*, pages 17–32, 2010.
- [135] Richard Booth, Thomas Meyer, Ivan José Varzinczak, and Renata Wassermann. Horn belief change: A contraction core. In *Proceedings of the 19th European Conference on Artificial Intelligence (ECAI 2010)*, pages 1065–1066, 2010.
- [136] Richard Booth, Yann Chevaleyre, Jérôme Lang, Jérôme Mengin, and Chattrakul Sombattheera. Learning conditionally lexicographic preference relations. In *Proceedings of the 19th European Conference on Artificial Intelligence (ECAI 2010)*, pages 269–274, 2010.
- [137] Richard Booth, Thomas Meyer, Ivan Varzinczak, and Renata Wassermann. A contraction core for horn belief change: Preliminary report. In *Proceedings of the 13th International Workshop on Non-Monotonic Reasoning (NMR 2010)*, 2010.
- [138] Emil Weydert. Ranking revision with conditional knowledge bases. In *Procs. of the 22nd Benelux Conference on Artificial Intelligence (BNAIC'10)*, 2010.
- [139] M.W.A. Caminada. Preferred semantics as socratic discussion. In *Proceedings of the eleventh AI*IA symposium on artificial intelligence*, pages 209–216, 2010.
- [140] Y. Wu, M. Podlaszewski, and M.W.A. Caminada. A labelling-based justification status of arguments. In *Proceedings of the 13th International Workshop on Non-Monotonic Reasoning (NMR)*, 2010.
- [141] Ch. Sakama and M.W.A. Caminada. The many faces of deception. In *Proceedings of the Thirty Years of Nonmonotonic Reasoning (Non-Mon30)*, 2010.

- [142] M.W.A. Caminada. An algorithm for stage semantics. In *Proceedings of the Third International Conference on Computational Models of Argument (COMMA 2010)*, pages 147–158, 2010.
- [143] M.W.A. Caminada and Y. Wu. On the justification status of arguments. In *Proceedings of the 22nd Benelux Conference on Artificial Intelligence*, 2010.
- [144] M.W.A. Caminada and B. Verheij. On the existence of semi-stable extensions. In *Proceedings of the 22nd Benelux Conference on Artificial Intelligence*, 2010.
- [145] Ch. Sakama, M.W.A. Caminada, and A. Herzig. A logical account of lying. In *Proceedings of the 12th European Conference on Logics in Artificial Intelligence (JELIA)*, volume 6341. 6341 of *Lecture Notes in Artificial Intelligence*, pages 286–299. Springer Berlin / Heidelberg, 2010.
- [146] Constantinos Papatheodorou, Antonis Bikakis, and Grigoris Antoniou. On the deployment of contextual reasoning in ambient intelligence environments. In *Intelligent Environments (IE)*, 2010.
- [147] Antonis Bikakis and Grigoris Antoniou. Contextual argumentation in ambient intelligence: Overview and future steps. In *Proceedings of the 4th Mahasarakham International Workshop on Artificial Intelligence (MIWAI'10)*, 2010.
- [148] Grigoris Antoniou, Antonis Bikakis, and Constantinos Papatheodorou. Reasoning with imperfect context and preference information reasoning with imperfect context and preference information in multi-context systems. In Barbara (Editor) Catania, Mirjana (Editor) Ivanovic, and Bernhard (Editor) Thalheim, editors, *Advances in Databases and Information Systems - 14th East European Conference, ADBIS 2010*, volume 6295. 6295 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2010.
- [149] Grigoris Antoniou, Constantinos Papatheodorou, and Antonis Bikakis. Reasoning about context in ambient intelligence environments: A report from the field. In Fangzhen (Editor) Lin, Ulrike (Editor) Sattler, and Mirosław (Editor) Truszczyński, editors, *Principles of Knowledge Representation and Reasoning: Proceedings of the Twelfth International Conference, KR 2010*. AAAI Press, 2010.
- [150] Antonis Bikakis and Grigoris Antoniou. Rule-based contextual reasoning in ambient intelligence. In Mike (Editor) Dean, John (Editor) Hall, Antonino (Editor) Rotolo, and Said (Editor) Tabet, editors, *Semantic Web Rules - International Symposium, RuleML 2010*, volume 6403.

- 6403 of *Lecture Notes in Computer Science*, pages 74–88. Springer, 2010.
- [151] Theodore Patkos, Ioannis Chryssakis, Antonis Bikakis, Dimitris Plexousakis, and Grigoris Antoniou. A reasoning framework for ambient intelligence. In Stasinou (Editor) Konstantopoulos, Stavros J. (Editor) Perantonis, Vangelis (Editor) Karkaletsis, Constantine D. (Editor) Spyropoulos, and George A. (Editor) Vouros, editors, *SETN*, volume 6040 of *Lecture Notes in Computer Science*, pages 213–222. Springer, 2010.
- [152] Antonis Bikakis and Grigoris Antoniou. Defeasible contextual reasoning in ambient intelligence: Theory and applications. In Robert (Editor) Meersman, Tharam S. (Editor) Dillon, and Pilar (Editor) Herero, editors, *OTM Workshops*, volume 6428. 6428 of *Lecture Notes in Computer Science*, page 89. Springer, 2010.
- [153] Maria Angeles Jurado Gallardo and Ghislain Ruy. Fm discriminator for ais satellite detection. In *Second International Conference on Personal Satellite Services (PSATS 2010)*, pages 19–34. Springer, 2010.
- [154] Baptiste Alcalde. Trusted third party, who are you? In *Short Paper Proceedings of the Fourth IFIP WG11.11 International Conference on Trust Management (IFIPTM 2010)*, pages 49–56. Information Processing Society of Japan, 2010.
- [155] W. Wei, X. Zhang, and G. Pitsilis. Abstracting audit data for efficient anomaly intrusion detection. In *Sixth International Conference on Information Systems Security (ICISS 2010)*, pages 201–215, Gandhinagar, India, December 2010.
- [156] R. Bakhshi, J. Endrullis, W. J. Fokkink, and Jun Pang. Brief announcement: Asynchronous bounded expected delay networks. In *Proc. 29th Annual ACM Symposium on Principles of Distributed Computing*, pages 392–393. ACM, 2010.
- [157] C. Zhang and J. Pang. On probabilistic alternating simulations. In *Proc. 6th IFIP Conference on Theoretical Computer Science*, volume 323. 323, pages 71–85. IFIP International Federation for Information Processing, 2010.
- [158] S. Mauw, S. Radomirovic, and P.Y. Ryan. Security protocols for secret santa. In *Proc. 18th Security Protocols Workshop*, Cambridge, March 2010.
- [159] J. Baeten, B. Luttik, T. Muller, and P. van Tilburg. Expressiveness modulo bisimilarity of regular expressions with parallel composition.

- In *Proc. 17th International Workshop on Expressiveness in Concurrency (EXPRESS'10 2010)*, pages 1–15, Paris, France, August 2010.
- [160] T. Muller. Semantics of trust. In *Proc. 7th Workshop on Formal Aspects in Security and Trust (FAST 2010)*, Lecture Notes in Computer Science, pages 141–156, Pisa, Italy, September 2010. Springer-Verlag.
- [161] N. Dong, H. L. Jonker, and J. Pang. Analysis of a receipt-free auction protocol in the applied pi calculus. In *Proc. 7th Workshop on Formal Aspects in Security and Trust*, volume 6561. 6561 of *Lecture Notes in Computer Science*, pages 223–238. Springer-Verlag, 2010.
- [162] Y. Sun, C. Zhang, J. Pang, B. Alcalde, and S. Mauw. A trust-augmented voting scheme for collaborative privacy management. In *Proc. 6th Workshop on Security and Trust Management*, Athens, Greece, September 2010.
- [163] Z. Liu, J. Pang, and C. Zhang. Extending a key-chain based certified email protocol with transparent ttp. In *Proc. 6th IEEE/IFIP Symposium on Trusted Computing and Communications*, pages 630–636. IEEE Computer Society, 2010.
- [164] Z. Liu, J. Pang, and C. Zhang. Verification of a key-chain based ttp transparent cem protocol. In *Proc. 4th Workshop on Harnessing Theories for Tool Support in Software (TTSS'2010)*, East China Normal University, Shanghai, November 2010.
- [165] F. Cassez, R. van der Meyden, and C. Zhang. The complexity of synchronous notions of information flow security. In *Proceedings of FoSSaCS 2010*, pages 282–296, 2010.
- [166] Hugo Jonker and Wolter Pieters. Anonymity in voting revisited. In *Towards Trustworthy Elections*, volume 6000. 6000 of *Lecture Notes in Computer Science*, pages 216–230. Springer, 2010.
- [167] Lucie Langer, Hugo Jonker, and Wolter Pieters. Anonymity and verifiability in voting: Understanding (un)linkability. In *Proc. ICICS*, Lecture Notes in Computer Science, pages 296–310. Springer-Verlag, 2010.
- [168] M. Torabi Dashti and S. Mauw. Fair exchange. In G. (Editor) Rosenberg, editor, *Handbook of Financial Cryptography and Security*, pages 109–132. Chapman and Hall/CRC, 2010.
- [169] Sasa Radomirovic. Towards a model for security and privacy in the internet of things. In *1st International Workshop on the Security of the Internet of Things (SecIoT'10)*, 2010.

- [170] T. van Deursen. 50 ways to break rfid privacy. In *Privacy and Identity Management for Life (PrimeLife 2010), PrimeLife/IFIP Summer School 2010*, Helsingborg, Sweden, August 2010.
- [171] W. Jamroga and N. Bulling. Comparing variants of strategic ability. In *Proceedings of EUMAS2010*, 2010.
- [172] V. Goranko, W. Jamroga, and P. Turrini. Strategic games and truly playable effectivity functions. In *Proceedings of EUMAS2010*, 2010.
- [173] M. Dastani and W. Jamroga. Reasoning about strategies of multi-agent programs. In *Proceedings of AAMAS2010*, pages 625–632, 2010.
- [174] N. Bulling and W. Jamroga. Verifying agents with memory is harder than it seemed. In *Proceedings of AAMAS2010*, pages 633–640, 2010.
- [175] N. Bulling, J. Dix, and W. Jamroga. Model checking logics of strategic ability: Complexity. In M. (Editor) Dastani, K. (Editor) Hindriks, and J.-J. (Editor) Meyer, editors, *Specification and Verification of Multi-Agent Systems*, pages 125–159. Springer, 2010.
- [176] Markus Esch and Ingo Scholtes. Resilience and multicast aspects of the structured network overlay gp3. In *Proceedings of International Conference on Complex, Intelligent and Software Intensive Systems (CISIS) 2010*, pages 117–122, 2010.
- [177] Johnatan E. Pecero, Sebastien Varrete, and Pascal Bouvry. Scheduling dag applications on multi-core processor packages architectures. In *International Conference on Metaheuristics and Nature Inspired Computing (Meta'10)*, pages 0–0, 2010.
- [178] Alex Biryukov, Deike Priemuth-Schmid, and Bin Zhang. Analysis of snow 3g+ resynchronization mechanism. In *SECRYPT 2010*, pages 327–333, 2010.
- [179] Barbara Kordy, Sjouke Mauw, Matthijs Melissen, and Patrick Schweitzer. Attack-defense trees and two-player binary zero-sum extensive form games are equivalent. In *Conference on Decision and Game Theory for Security (GameSec 2010)*, volume 6442 LNCS, pages 245–256. Springer, 2010.
- [180] Marcin Sredynski and Pascal Bouvry. Trust management for collusion prevention in mobile ad hoc networks. In *Proc. IEEE Globecom 2010 Workshop on Management of Emerging Networks and Services*, pages 523–528. IEEE, 2010.
- [181] Marcin Sredynski and Pascal Bouvry. The cost of altruistic punishment in indirect reciprocity-based cooperation in mobile ad hoc

- networks. In *Proc. Sixth IEEE/IFIP International Symposium on Trusted Computing and Communications (TrustCom 2010) in conjunction with EUC-10*, pages 749–755, 2010.
- [182] Marcin Seredynski and Pascal Bouvry. Free riding-based energy saving in mobile ad hoc networks. In *Proc. International Conference on Metaheuristics and Nature Inspired Computing (META 2010)*, pages 1–2, 2010.
- [183] Marcin Seredynski and Pascal Bouvry. Direct vs. indirect reciprocity trust system in ad hoc networks. In *Proc. 4th IFIP WG 11.11 International Conference on Trust Management (short paper), IFIPTM 2010, Morioka, Japan*, pages 111–118, 2010.
- [184] Julien Schleich, Grégoire Danoy, Pascal Bouvry, and Hoai An Le Thi. On quantifying the quality of cds-based virtual backbones in mobile ad hoc networks. In *Proc. 8th ACM International Symposium on Mobility Management and Wireless Access*, pages 21–28, 2010.
- [185] Pascal Bouvry Patricia Ruiz. Distributed energy self-adaptation in ad hoc networks. In *IEEE International workshop on Management of Emerging Networks and Services (MENS), in conjunction with IEEE Globecom*, pages 539–543. IEEE, 2010.
- [186] Jean Botev and Ingo Scholtes. A resource allocation scheme for decentralized distributed virtual environments. In *Proceedings of the 6th International Conference on Collaborative Computing*, pages 0 – 0, 2010.
- [187] Markus Esch and Jean Botev. Distance-aware avatar interaction in online virtual environments. In *Proceedings of the 2nd International Conference on Advances in Future Internet*, pages 56 – 62, 2010.
- [188] Nuno Amalio and Pierre Kelsen. Vcl, a visual language for abstract specification of software systems formally and modularly. In *Diagrams 2010*, volume 6170. 6170 of *LNCS*, pages 6170–282. Springer, 2010.
- [189] Nuno Amalio, Pierre Kelsen, and Qin Ma. Specifying structural properties and their constraints formally, visually and modularly using vcl. In *EMMSAD 2010*, volume 50. 50 of *LNBIP*, pages 50–261. Springer, 2010.
- [190] Nuno Amalio and Pierre Kelsen. Modular design by contract visually and formally using vcl. In *VL/HCC 2010*. IEEE, 2010.
- [191] Andreas Rusnjak, Hristomir Hristov, Marwane El Kharbili, and Andreas Speck. Managing the dynamics of em commerce with a hierarchical overlapping business-value framework. In *The 6th international*

- Symposium on Web and Mobile Information Services (WAMIS 2010)*, 2010.
- [192] Nicolas Guelfi, Cedric Pruski, and Chantal Reynaud. Experimental assessment of the target adaptive ontology-based web search framework. In NULL (Editor), editor, *NOTERE'2010*, 2010.
- [193] Bruno Barroca, Levi Lucio, Vasco Amaral, Roberto Felix, and Vasco Sousa. Dsltrans: A turing incomplete transformation language. In *Software Language Engineering*. LNCS, 2010.
- [194] M. Szaban, J. P. Nowacki, A. Drabik, F. Seredynski, and P. Bouvry. Application of cellular automata in symmetric key cryptography. In *Advances in Information Technology*, volume 114, pages 154–163. Springer CCIS, 2010.
- [195] Ton van Deursen and Sasa Radomirovic. Ec-rac: Enriching a capacious rfid attack collection. In *6th Workshop on RFID Security (RFIDSec 2010)*, volume 6370, pages 75–90. Springer, 2010.
- [196] Ileana Buhan, Gabriele Lenzini, and Sasa Radomirovic. Contextual biometric-based authentication for ubiquitous services. In *7th International Conference on Ubiquitous Intelligence and Computing (UIC 2010)*, volume 6406, pages 680–693. Springer, 2010.
- [197] Shaonan Wang, Radu State, Mohamed Ourdane, and Thomas Engel. Riskrank: Security risk ranking for ip flow records. In *Proceedings of the 2010 International Conference on Network and Services Management*, pages 56–63, 2010.
- [198] Cynthia Wagner, Gerard Wagener, Radu State, Alexandre Dulaunoy, and Thomas Engel. Peekkernelflows: Peeking into ip flows. In *VizSec '10 Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, pages 52–57. ACM, 2010.
- [199] Radha Thangaraj, Millie Pant, Pascal Bouvry, and Ajith Abraham. Evolutionary algorithms for solving stochastic programming problems. In *Int. Conf. on Computational Intelligence Communication Networks (CICN 2010)*, pages 628–632. IEEE Computer Society Press, 2010.
- [200] Frederic Pinel, Bernabe Dorronsoro, and Pascal Bouvry. A new cellular genetic algorithm designed for the gpu to solve the scheduling problem. In *META*, pages 0–0, 2010.
- [201] Radha Thangaraj, Millie Pant, Pascal Bouvry, and Ajith Abraham. Solving multi objective stochastic programming problems using differential evolution. In *Lecturer Notes in Computer Science (LNCS)*, volume 6466, pages 54 – 61. Springer, 2010.

- [202] Yoann Pigne, Gregoire Danoy, and Pascal Bouvry. A platform for realistic online vehicular network management. In *International Workshop on Management of Emerging Networks and Services (MENS 2010) in conjunction with IEEE GLOBECOM 2010*, pages 1–5, 2010.
- [203] J. Alberto Dorronsoro, Bernabeand Canero, Gregoire Danoy, and Pascal Bouvry. A new parallel multi-objective cooperative coevolutionary algorithm based on spea2. In *ALIO-INFORMS Joint International Meeting 2010 (2010)*, pages 0–2, 2010.
- [204] Pascal Dorronsoro, Bernabeand Bouvry and Enrique Alba. Iterated local search for de novo genomic sequencing. In *10th International Conference on Artificial Intelligence and Soft Computing (ICAISC), Lecture Notes in Artificial Intelligence (LNAI) series*, volume 6114, pages 428–436. Springer-Verlag, 2010.
- [205] Radha Thangaraj, Thanaga Raj Chelliah, Pascal Bouvry, Millie Pant, and AJith Abraham. Optimal design of induction motor for a spinning machine using population based metaheuristics. In *Int. Conf. on Computer Information Systems and Industrial Management Applications*, pages 341–346. IEEE Computer Society Press, 2010.
- [206] Pascal Dorronsoro, Bernabeand Bouvry, J. Alberto Canero, Anthony A. Maciejewski, and Howard Jay Siegel. Multi-objective robust static mapping of independent tasks on grids. In *Proceedings of the IEEE Congress on Evolutionary Computation (CEC), part of World Conference in Computational Intelligence (WCCI)*, pages 3389–3396. IEEE, 2010.
- [207] Jayanta Poray and Christoph Schommer. Managing conversational streams by explorative mind-maps. In *Computer Systems and Applications (AICCSA), 2010 IEEE/ACS International Conference*, pages 1 – 4, 2010.
- [208] Kenneth Sebesta, Nicolas Boizot, Eric Busvelle, and Jurgen Sachau. Using an adaptive high-gain extended kalman filter with a car efficiency model. In *Proceedings of 3rd Annual Dynamic Systems and Control Conference*, pages 0–0, Cambridge, Massachusetts, USA, September 2010.
- [209] Johnatan E. Pecero and Pascal Bouvry. An improved genetic algorithm for efficient scheduling on distributed memory parallel systems. In *Computer Systems and Applications (AICCSA), 2010 IEEE/ACS International Conference on*, pages 1 – 8. IEEE, 2010.
- [210] Xiangliang Zhang, Wei Wang, Kjetil Nørnvåg, and Michele Sebag. K-ap: Generating specified k clusters by efficient affinity propagation.

- In *Proceedings of the tenth IEEE International Conference on Data Mining (ICDM' 2010)*, pages 1187–1192, Sydney, Australia, December 2010. IEEE Computer Society.
- [211] Xiangliang Zhang and Wei Wang. Self-adaptive change detection in streaming data with non-stationary distribution. In *Proceedings of the 6th International Conference on Advanced Data Mining and Applications (ADMA' 2010)*, volume 6440, pages 334–345. Springer 2010, 2010.
- [212] Jorn-Marc Schmidt, Michael Tunstall, Roberto Avanzi, Ilya Kizhvatov, Timo Kasper, and David Oswald. Combined implementation attack resistant exponentiation. In *Progress in Cryptology - LATIN-CRYPT 2010*, volume 6212, pages 305 – 322. Springer, 2010.
- [213] Jean-Sebastien Coron and Ilya Kizhvatov. Analysis and improvement of the random delay countermeasure of ches 2009. In *Cryptographic Hardware and Embedded Systems - CHES 2010*, volume 6225, pages 95 – 109. Springer, 2010.
- [214] Sheila Becker, Humberto Abdelnur, Jorge Lucangeli Obes, Radu State, and Olivier Festor. Improving fuzz testing using game theory. In *Proceedings of the 2010 Fourth International Conference on Network and System Security (NSS'2010)*, pages 263–268, Washington, DC, USA, 2010. IEEE Computer Society.
- [215] Sheila Becker, Humberto Abdelnur, Radu State, and Thomas Engel. An autonomic testing framework for ipv6 configuration protocols. In *Mechanisms for Autonomous Management of Networks and Services*, pages 65 – 76. Springer, 2010.
- [216] Mateusz Guzek, Johnatan E. Pecero, Bernabe Dorronsoro, Pascal Bouvry, and Samee U. Khan. A cellular genetic algorithm for scheduling applications and energy-aware communication optimization. In *High Performance Computing and Simulation (HPCS), 2010 International Conference on*, pages 241–248, 2010.
- [217] Shaonan Wang, Radu State, Mohamed Ourdane, and Thomas Engel. Mining netflow records for critical network activities. In *Mechanisms for Autonomous Management of Networks and Services, 4th International Conference on Autonomous Infrastructure, Management and Security*, volume 6155, pages 135–146. Springer, 2010.
- [218] Shaonan Wang, Radu State, Mohamed Ourdane, and Thomas Engel. Flowrank: Ranking netflow records. In *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference, IWCMC 2010*,, pages 484–488. ACM, 2010.

- [219] Raphael Frank, Eugenio Giordano, Pasquale Cataldi, and Mario Gerla. Trafroute: A different approach to routing in vehicular networks. In *1st International Workshop on Vehicular Communications and Networking (VECON'2010)*, pages 521–528, Niagara Falls, Ontario, Canada, October 2010.
- [220] Eugenio Giordano, Raphael Frank, Giovanni Pau, and Mario Gerla. Corner: A step towards realistic simulations for vanet. In *Proceedings of The Seventh ACM International Workshop on Vehicular Inter-Networking (VANET 2010)*., pages 41–50, Chicago, Illinois, USA, 2010. ACM.
- [221] Eugenio Giordano, Raphael Frank, Giovanni Pau, and Mario Gerla. Corner: a realistic urban propagation model for vanet. In *Proceedings of Seventh IEEE International Conference on Wireless On-demand Network Systems and Services (WONS 2010)*, pages 99–105, 2010.
- [222] Raphael Frank, Thomas Scherer, and Mario Gerla. Edfs a novel flooding protocol for multi-hop wireless networks. In *Proceedings of IEEE WONS 2010 Seventh International Conference on Wireless On-demand Network Systems and Services*, pages 349–354, 2010.
- [223] Cynthia Wagner, Gerard Wagener, Radu State, Alexandre Dulaunoy, and Thomas Engel. Breaking tor anonymity with game theory and data mining. In *Proceedings of 4th International Conference on Network and System Security NSS2010*, pages 47–54. IEEE, 2010. Best Paper Award of NSS 2010.
- [224] Frederic I Pinel, Johnatan Pecero, Pascal Bouvry, and Samee Khan. Memory-aware green scheduling on multi-core processors. In *Proceedings of the 2010 39th International Conference on Parallel Processing Workshops (ICPPW '10)*, pages 485–488. IEEE Computer Society, 2010.
- [225] Yoann Pigne and Frederic Guinand. Short and robust communication paths in dynamic wireless networks. In *ANTS 2010*, volume LNCS 6234, pages 520 – 527. Springer, Heidelberg, 2010.
- [226] Gabriel Sandulescu and Simin Nadjm-Tehrani. Optimising replication versus redundancy in window-aware opportunistic routing. In *Proceedings of the third international Conference on Communication Theory, Reliability, and Quality of Service (CTRQ '10)*, pages 192–201. IEEE Computer Society, 2010.
- [227] Frederic Pinel, Bernabe Dorronsoro, and Pascal Bouvry. On the parallelization of asynchronous cellular genetic algorithms for multi-core

- architectures. In *ALIO-INFORMS Joint International Meeting 2010*, pages 0–2, 2010.
- [228] Yoann Pigne, Arnaud Casteigts, Frederic Guinand, and Serge Chaumette. Construction et maintien d’une forêt couvrante dans un reseau dynamique. In *12emes Rencontres Francophones sur les Aspects Algorithmiques de Telecommunications (AlgoTel)*, pages 67 – 70, 2010.
- [229] Patricia Ruiz and Pascal Bouvry. Enhanced distance based broadcasting protocol with reduced energy consumption. In *IEEE International Conference on High Performance Computing & Simulation*, pages 249–258. IEEE, 2010.
- [230] Frederic Pinel, Bernabe Dorronsoro, and Pascal Bouvry. A new parallel asynchronous cellular genetic algorithm for scheduling in grids. In *IPDPS Workshops*, pages 1–8, Atlanta, Georgia, USA, April 2010. IEEE.
- [231] Miguel Couceiro and Erkkko Lehtonen. Explicit descriptions of bisymmetric sugeno integrals. In *Computational Intelligence for Knowledge-Based Systems Design, Lecture Notes in Artificial Intelligence*, volume 6178, pages 494–501. Springer-Verlag, 2010.
- [232] Eugen Staab and Martin Caminada. On the profitability of incompetence. In *Proc. of the 11th Int. Workshop on Multi-Agent-Based Simulation (MABS 2010)*, pages 1–15, 2010.
- [233] Gilles Perrouin, Sagar Sen, Jacques Klein, Benoit Baudry, and Yves Le Traon. Automated and scalable t-wise test case generation strategies for software product lines. In *Proceedings of the 2010 Third International Conference on Software Testing, Verification and Validation (ICST’2010)*, pages 459–468. IEEE Computer Society, 2010.
- [234] Miguel Couceiro and Erkkko Lehtonen. Classes of operations closed under permutation, cylindrification and composition. In *40th IEEE International Symposium on Multiple-Valued Logic (ISMVL 2010)*, pages 117–121. IEEE Computer Society, 2010.
- [235] Miguel Couceiro and Erkkko Lehtonen. The arity gap of polynomial functions over bounded distributive lattices. In *40th IEEE International Symposium on Multiple-Valued Logic (ISMVL 2010)*, pages 113–116. IEEE Computer Society, 2010.
- [236] David Fotue, Foued Melakessou, Houda Labiod, and Thomas Engel. Design of an enhanced energy conserving routing protocol based on route diversity in wireless sensor networks. In *The 9th IEEE/IFIP*

- Annual Mediterranean Ad Hoc Networking Workshop*, pages 1–6. IEEE Xplore, 2010.
- [237] X. An and Jun Pang. Model checking round-based distributed algorithms. In IEEE, editor, *Proc. 15th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 2010)*, pages 127–135, Oxford, United Kingdom, March 2010.
- [238] Maria Angeles, Jurado Gallardo, and Ghislain Ruy. Novel demodulator for spaceborne ais reception with increased robustness against noise. In *Signal Processing, Pattern Recognition and Applications*, 2010.
- [239] MM. A. Jurado Gallardo and Ulrich Sorger. Coherent receiver for ais satellite detection. In *4th International Symposium on Communications, Control and Signal Processing (ISCCSP)*, 2010.
- [240] Jean-Sébastien Coron, Yevgeniy Dodis, Avradip Mandal, and Yannick Seurin. A domain extender for the ideal cipher. In *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings*, volume 5978, pages 273–289. Springer, 2010.
- [241] Sascha Kaufmann and Christoph Schommer. Towards e-conviviality in web-based systems by considering the wisdom of crowds. In *2nd Conference on Agents and Artificial Intelligence*, pages 305 – 307, 2010.
- [242] Christoph Schommer. A molecular concept of managing data. In *2nd Conference on Agents and Artificial Intelligence (ICAART 2010)*, pages 300–305, 2010.
- [243] Frederic Pinel and Pascal Bouvry. Weakness analysis of a key stream generator based on cellular automata. In *Parallel Processing and Applied Mathematics (Proc. Parallel Processing and Applied Mathematics (PPAM 2009))*, Springer LNCS, LNCS. Springer Verlag, 2010.

7.6 PhD Thesis

- [244] Raphael Frank. *Efficient Data Dissemination Techniques for Multi-Hop Wireless Networks Applied to Vehicular Communications*. PhD thesis, University of Luxembourg, July 2010.
- [245] Nicolas Boizot. *Adaptive High-gain Extended Kalman Filter and Applications*. PhD thesis, 2010.

- [246] Alfredo Capozucca. *DT4BP: a Business Process Modelling Language for Dependable Time-Constrained Business Processes*. PhD thesis, 2010.
- [247] Kenneth Sebesta. *Optimal Observers and Optimal Control: Improving Car Efficiency with Kalman and Pontryagin*. PhD thesis, 2010.
- [248] Barbara Gallina. *PRISMA: a Software Product Line-oriented Process for the Requirements Engineering of Flexible Transaction Models*. PhD thesis, 2010.

7.7 Internal Reports

- [249] Nicolas Guelfi. A formal framework for dependability and resilience from a software engineering perspective. Technical Report TR-LASSY-10-01, University of Luxembourg, 2010.
- [250] Pierre Kelsen, Qin Ma, and Christian Glodt. A generic model decomposition technique. Technical Report TR-LASSY-10-06, University of Luxembourg, 2010.
- [251] Levi Lúcio and Nicolas Guelfi. A precise definition of operational resilience. Technical Report TR-LASSY-11-02, Laboratory for Advanced Software Systems, University of Luxembourg, 2011.
- [252] Federico Wiecko. An evaluation of mde tools in the context of m2m transformations. Technical Report TR-LASSY-10-04, University of Luxembourg, 2010.
- [253] Ayda Saidane. Dref resiliency and security aspects in the sae architecture analysis and design language (aadl). Technical Report TR-LASSY-10-07, University of Luxembourg, 2010.
- [254] Yiqing Li. Model-driven development of crisis management application in software product line approach. Technical Report TR-LASSY-10-05, Laboratory for Advanced Software Systems, University of Luxembourg, 2010.
- [255] Gilles Perrouin and Ayda Saidane. State of the art in architecture description languages for resiliency and security specification. Technical Report TR-LASSY-10-02, University of Luxembourg, 2010.
- [256] Nuno Amalio and Pierre Kelsen. the visual contract language: abstract modelling of software systems visually, formally and modularly. Technical Report TR-LASSY-10-03, University of Luxembourg, 2010.

7.8 Proceedings

- [257] Pompeu Casanovas, Ugo Pagallo, Giovanni Sartor, and Gianmaria Ajani, editors. *AI Approaches to the Complexity of Legal Systems. Complex Systems, the Semantic Web, Ontologies, Argumentation, and Dialogue - International Workshops AICOL-I/IVR-XXIV Beijing, China, September 19, 2009 and AICOL-II/JURIX 2009, Rotterdam, The Netherlands, December 16, 2009 Revised Selected Papers*, volume 6237 of *Lecture Notes in Computer Science*. Springer, 2010.
- [258] Carles Sierra, Cristiano Castelfranchi, Keith S. Decker, and Jaime Simão Sichman, editors. *8th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS 2009), Budapest, Hungary, May 10-15, 2009, Volume 2*. IFAAMAS, 2009.
- [259] Julian A. Padget, Alexander Artikis, Wamberto Weber Vasconcelos, Kostas Stathis, Viviane Torres da Silva, Eric T. Matson, and Axel Polleres, editors. *Coordination, Organizations, Institutions and Norms in Agent Systems V, COIN 2009 International Workshops. COIN@AAMAS 2009, Budapest, Hungary, May 2009, COIN@IJCAI 2009, Pasadena, USA, July 2009, COIN@MALLOW 2009, Turin, Italy, September 2009. Revised Selected Papers*, volume 6069 of *Lecture Notes in Computer Science*. Springer, 2010.
- [260] V. Goranko and W. Jamroga, editors. *Proceedings of the 3rd Workshop on Logical Aspects of Multi-Agent Systems (LAMAS 2010)*. IFAAMAS, 2010.
- [261] J. Dix, J. Leite, G. Governatori, and W. Jamroga, editors. *Computational Logic in Multi-Agent Systems. Proceedings of CLIMA XI*, volume 6245 of *Lecture Notes in Computer Science*. Springer, 2010.

Acronyms used

ComSys Communicative Systems Laboratory

CSC Computer Science & Communications

HPC High Performance Computing

ILIAS Interdisciplinary Laboratory for Intelligent and Adaptive Systems

LACS Laboratory of Algorithmics, Cryptology and Security

LASSY Laboratory for Advanced Software Systems

SnT Interdisciplinary Centre for Security Reliability and Trust

UL University of Luxembourg

<http://csc.uni.lu>

Computer Science & Communication (CSC) Research Unit
University of Luxembourg
Faculty of Science, Technology and Communication
6, rue Richard Coudenhove-Kalergi
L-1359 Luxembourg
Luxembourg

Administrative Contact:

Isabelle Glemot-Schroeder and Fabienne Schmitz
Email: csc@uni.lu