IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2014

Project-Team MADYNES

Management of dynamic networks and services

IN COLLABORATION WITH: Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

RESEARCH CENTER
Nancy - Grand Est

THEME
Networks and Telecommunications

Table of contents

Project-Team MADYNES

Keywords: Ambient Computing, Monitoring, Network Protocols, Peer-to-peer, Security, Self-management

Creation of the Project-Team: 2004 February 01.

1. Members

Research Scientists

Jérôme François [Inria, Researcher]
Vassili Rivron [Inria, Researcher (Assistant Professor en détachement from University of Caen since September 2013)]

Faculty Members

Olivier Festor [Team leader until June 2014, Univ. Lorraine, Professor, HdR]
Isabelle Chrisment [Team leader since July 2014, Univ. Lorraine, Professor, HdR]
Bernardetta Addis [Univ. Lorraine, Associate Professor]
Laurent Andrey [Univ. Lorraine, Associate Professor]
Rémi Badonnel [Univ. Lorraine, Associate Professor]
Thibault Cholez [Univ. Lorraine, Associate Professor]
Laurent Ciarletta [Univ. Lorraine, Associate Professor]
Abdelkader Lahmadi [Univ. Lorraine, Associate Professor]
Emmanuel Nataf [Univ. Lorraine, Associate Professor]
Thomas Silverston [Univ. Lorraine, Associate Professor until Sep. 2014 (currently in CNRS delegation at JFLI, University of Tokyo, Japan)]
Françoise Simonot-Lion [Univ. Lorraine, Professor Emerite]
Ye-Qiong Song [Univ. Lorraine, Professor, HdR]

Engineers

Eric Finickel [Inria, ADT SEA, since Nov 2013]
Florian Greff [Univ. Lorraine, from Nov 2014]
Adrien Guenard [Univ. Lorraine, granted by Hydradrone project from R&D Lorraine project]
Ceilidh Hoffmann [Inria, ADT R2D2, since Mar 2014]
Mohammad Irfan Khan [Inria, ADT Metrocope, since Nov 2013]
Yannick Presse [Inria, granted by EDF]
Benjamin Segault [Inria, granted by EDF, from Oct 2014]
Mandar Harshe [Univ. Lorraine, granted by SATELOR project from AME Lorraine, since Jan 2014]

PhD Students

Elian Aubry [Univ. Lorraine, granted by Ministry of Research, since Oct 2013]
Martin Barrere [Inria, granted by FP7 UNIVERSELF project, from Mar 2011 to Mar 2014]
César Bernardini [Inria, granted by FP7 UNIVERSELF project and Conseil Régional de Lorraine, since Nov 2011]
François Despaux [Univ. Lorraine, granted by ANR QUASIMODO, since Oct 2011]
Patrick-Olivier Kamgueu [Univ. Lorraine, granted by Ministry of Foreign Affairs, since Jun 2012, in co-supervision with Université de Yaounde]
Anthéa Mayzaud [Inria, granted by FP7 FLAMINGO and Conseil Régional de Lorraine, since May 2013]
Kévin Roussel [Inria, granted by LAR project from PIA, since Dec 2012]
Mohamed Said Seddiki [Univ. Lorraine, granted by the Tunisian Ministry of Research, in co-supervision with SupCom Tunis, since Mar 2013]
Shbair Wazen [Univ. Lorraine, granted by Erasmus Mundus EPIC, since Dec. 2013]
Evangelia Tsiontsiou [Univ. Lorraine, granted by SATELOR project from AME Lorraine, since Oct 2013]

Gaëtan Hurel [Inria, granted by FP7 FLAMINGO, since Jan 2014]
Samuel Marchal [Univ. Lorraine, co-tutelle with Univ. Luxembourg, since October 2011]

Visiting Scientists

Raouf Boutaba [Univ. of Waterloo, Canada, from Jul 2014 until Aug 2014]
Lamia Fourati-Chaari [Institut d'Informatique et de Multimédia de Sfax (Tunisie), Assistant Professor, Jun 2014]
Celia Ouanteur [PhD Student, from May 2014 until Jun 2014]
Xiufang Shi [PhD student, from Mar 2014 until Jun 2014]
Shuguo Zhuo [PhD student, from May until Aug 2014]

Administrative Assistants

Isabelle Herlich [Inria]
Delphine Hubert [Univ. Lorraine]
Martine Kuhlmann [CNRS]

Others

Pedro Paulo Martins Dos Santos [Inria, Intern from Universidade de Brasília, Brazil, from Jun 2014 until Aug 2014]
Juan Pablo Timpanaro [Univ. Lorraine, ATER until Aug 2014]
Younes Abid [Univ. Lorraine, Master student, until Jul 2014]
Ronny Chevalier [Inria, Intern from ENS Rennes, from May 2014 until Jul 2014]
Dragos Costea [Univ. Lorraine, Intern from Supelec, from Apr 2014 until Sep 2014]
Anthony Deroche [Inria, Intern from Telecom Nancy, from Jun 2014 until Aug 2014]
Thierry Duhal [Inria, Intern from Telecom Nancy, from Jun 2014 until Aug 2014]
Arthur Garnier [Inria, intern from IUT Charlemagne, from Apr 2014 until Jun 2014]
Antoine Goichot [Inria, Intern from Telecom Nancy, from Jun 2014 until Aug 2014]
Maxence Ho [Univ. Lorraine, Intern from MinesNancy, from Jun 2014 until Sep 2014]
Hubert Kenfack Ngankam [Inria, Intern from LIRIMA, from June until Aug 2014]
Yael Kolasa [Univ. Lorraine, Intern from Telecom Nancy, from Jun 2014 until Aug 2014]
Paulo Matias [Univ. Lorraine, Intern from ENSEM, from November 2013 until February 2014]
Martin Thiriau [Univ. Lorraine, Intern from Mines Nancy, from Jun 2014 until Sep 2014]
Fadhlallah Saddam Baklouti [Inria, Intern from ENSI-Tunis, from Apr 2014 until Sep 2014]
Raphael Cherfan [Univ. Lorraine, Intern from ESSTIN, from Apr 2014]
Alexandre Roux [Univ. Lorraine / TELECOM Nancy, Master Student, from Mar 2014 until Aug 2014]

2. Overall Objectives

2.1. Overall Objectives

The goal of the MADYNES research group is to design, to validate and to deploy novel management and security paradigms together with supporting software architectures and solutions that are able to cope with the growing dynamicity and the scalability issues induced by the ubiquitous Internet.

The project develops applied research activities in the following areas:

- **Autonomous Management**:
  - the design of models and methods enabling *self-organization and self-management* of networked entities and services,
  - the evaluation of management architectures based on *peer-to-peer and overlay principles*,
  - the investigation of novel approaches to the representation of *management information*,
  - the modeling and *performance evaluation* of dynamic networks.
- **Functional Areas** instantiate autonomous management functions:

- the *security plane* where we focus on building closed-loop approaches to protect networking assets,
- the *service configuration* where we aim at providing solutions covering the delivery chain from device discovery to QOS-aware delivery in dynamic networks,
- *monitoring* where we aim at building solutions to characterize and detect unwanted service behavior.

The next generation Internet is the main application field of our research. Its architecture and the services that it is planned to support offer all dynamic and scalability features that we address in the complementary research directions of the project.

3. Research Program

3.1. Evolutionary needs in network and service management

The foundation of the MADYNES research activity is the ever increasing need for automated monitoring and control within networked environments. This need is mainly due to the increasing dependency of both people and goods towards communication infrastructures as well as the growing demand towards services of higher quality. Because of its strategic importance and crucial requirements for interoperability, the management models were constructed in the context of strong standardization activities by many different organizations over the last 15 years. This has led to the design of most of the paradigms used in today's deployed approaches. These paradigms are the Manager/Agent interaction model, the Information Model paradigm and its container, together with a naming infrastructure called the Management Information Base. In addition to this structure, five functional areas known under Fault, Configuration, Accounting, Performance and Security are associated to these standards.

While these models were well suited for the specific application domains for which they were designed (telecommunication networks or dedicated protocol stacks), they all show the same limits. Especially they are unable:

1. to deal with any form of dynamicity in the managed environment,
2. to master the complexity, the operating mode and the heterogeneity of the emerging services,
3. to scale to new networks and service environments.

These three limits are observed in all five functional areas of the management domain (fault, configuration, accounting, performance and security) and represent the major challenges when it comes to enable effective automated management and control of devices, networks and services in the next decade.

MADYNES addresses these challenges by focusing on the design of management models that rely on inherently dynamic and evolving environments. The project is centered around two core activities. These activities are, as mentioned in the previous section, the design of an autonomous management framework and its application to three of the standard functional areas namely security, configuration and performance.

3.2. Autonomous management

3.2.1. Models and methods for a self-management plane

Self organization and automation are fundamental requirements within the management plane in today's dynamic environments. It is necessary to automate the management processes and enable management frameworks to operate in time sensitive evolving networks and service environments. The automation of the organization of devices, software components, networks and services is investigated in many research projects and has already led to several solution proposals. While these proposals are successful at several layers, like IP auto-configuration or service discovery and binding facilities, they did not enhance the management plane at all. For example, while self-configuration of IP devices is commonplace, no solution exists that provides strong support to the management plane to configure itself (e.g. finding the manager to which an agent has to send traps or organizing the access control based on locality or any other context information). So, this area represents a major challenge in extending current management approaches so that they become self-organized.

Our approach is bottom-up and consists in identifying those parameters and framework elements (manager data, information model sharing, agent parameters, protocol settings, ...) that need dynamic configuration and self-organization (like the address of a trap sink). For these parameters and their instantiation in various management frameworks (SNMP, Netconf, WBEM, ...), we investigate and elaborate novel approaches enabling fully automated setup and operation in the management plane.

3.2.2. Design and evaluation of P2P-based management architectures

Over the last years, several models have emerged and gained wide acceptance in the networking and service world. Among them, the overlay networks together with the P2P paradigms appear to be very promising. Since they rely mainly on fully decentralized models, they offer excellent fault tolerance and have a real potential to achieve high scalability. Mainly deployed in the content delivery and the cooperation and distributed computation disciplines, they seem to offer all features required by a management framework that needs to operate in a dynamic world. This potential however needs an in depth investigation because these models have also many characteristics that are unusual in management (e.g. a fast and uncontrolled evolution of the topology or the existence of a distributed trust relationship framework rather than a standard centralized security framework).

Our approach envisions how a complete redesign of a management framework is done given the characteristics of the underlying P2P and overlay services. Among the topics of interest we study the concept of management information and operations routing within a management overlay as well as the distribution of management functions in a multi-manager/agent P2P environment. The functional areas targeted in our approach by the P2P model are network and service configuration and distributed monitoring. The models are to be evaluated against highly dynamic frameworks such as ad-hoc environments (network or application level) and mobile devices.

3.2.3. Integration of management information

Representation, specification and integration of management information models form a foundation for network and service management and remains an open research domain. The design and specification of new models is mainly driven by the appearance of new protocols, services and usage patterns. These need to be managed and exposed through well designed management information models. Integration activities are driven by the multiplication of various management approaches. To enable automated management, these approaches need to inter-operate which is not the case today.

The MADYNES approach to this problem of modeling and representation of management information aims at:

1. enabling application developers to establish their management interface in the same workspace, with the same notations and concepts as the ones used to develop their application,
2. fostering the use of standard models (at least the structure and semantics of well defined models),
3. designing a naming structure that allows the routing of management information in an overlay management plane, and
4. evaluating new approaches for management information integration especially based on management ontologies and semantic information models.

3.2.4. Modeling and benchmarking of dynamic networks

The impact of a management approach on the efficiency of the managed service is highly dependent on three factors:

- the distribution of the considered service and their associated management tasks,
- the management patterns used (e.g. monitoring frequency, granularity of the management information considered),
- the cost in terms of resources these considered functions have on the managed element (e.g. method call overhead, management memory footprint).

MADYNES addresses this problem from multiple viewpoints: communication patterns, processing and memory resources consumption. Our goal is to provide management patterns combining optimized management technologies so as to optimize the resources consumed by the management activity imposed by the operating environment while ensuring its efficiency in large dynamic networks.

3.3. Functional areas

3.3.1. Security management

Securing the management plane is vital. While several proposals are already integrated in the existing management frameworks, they are rarely used. This is due to the fact that these approaches are completely detached from the enterprise security framework. As a consequence, the management framework is "managed" separately with different models; this represents a huge overhead. Moreover the current approaches to security in the management plane are not inter-operable at all, multiplying the operational costs in a heterogeneous management framework.

The primary goal of the research in this activity is the design and the validation of a security framework for the management plane that will be open and capable to integrate the security services provided in today's management architectures. Management security interoperability is of major importance in this activity.

Our activity in this area aims at designing a generic security model in the context of multi-party / multi-technology management interactions. Therefore, we develop research on the following directions:

1. Abstraction of the various access control mechanisms that exist in today's management frameworks. We are particularly interested in extending these models so that they support event-driven management, which is not the case for most of them today.
2. Extension of policy and trust models to ease and to ensure coordination among managers towards one agent or a subset of the management tree. Provisional policies are of great interest to us in this context.
3. Evaluation of the adequacy of key distribution architectures to the needs of the management plane as well as selecting reputation models to be used in the management of highly dynamic environments (e.g. multicast groups, ad-hoc networks).

A strong requirement towards the future generic model is that it needs to be instantiated (with potential restrictions) into standard management platforms like SNMP, WBEM or Netconf and to allow interoperability in environments where these approaches coexist and even cooperate. A typical example of this is the security of an integration agent which is located in two management worlds.

Since 2006 we have also started an activity on security assessment. The objective is to investigate new methods and models for validating the security of large scale dynamic networks and services. The first targeted service is VoIP.

3.3.2. Configuration: automation of service configuration and provisioning

Configuration covers many processes which are all important to enable dynamic networks. Within our research activity, we focus on the operation of tuning the parameters of a service in an automated way. This is done together with the activation topics of configuration management and the monitoring information collected from the underlying infrastructure. Some approaches exist today to automate part of the configuration process (download of a configuration file at boot time within a router, on demand code deployment in service platforms). While these approaches are interesting they all suffer from the same limits, namely:

1. they rely on specific service life cycle models,
2. they use proprietary interfaces and protocols.

These two basic limits have high impacts on service dynamics in a heterogeneous environment.

We follow two research directions in the topic of configuration management. The first one aims at establishing an abstract life-cycle model for either a service, a device or a network configuration and to associate with this model a generic command and programming interface. This is done in a way similar to what is proposed in the area of call control in initiatives such as Parlay or OSA.

In addition to the investigation of the life-cycle model, we work on technology support for distributing and exchanging configuration management information. Especially, we investigate policy-driven approaches for representing configurations and constraints while we study XML-based protocols for coordinating distribution and synchronization. Off and online validation of configuration data is also part of this effort.

3.3.3. Performance and availability monitoring

Performance management is one of the most important and deployed management function. It is crucial for any service which is bound to an agreement about the expected delivery level. Performance management needs models, metrics, associated instrumentation, data collection and aggregation infrastructures and advanced data analysis algorithms.

Today, a programmable approach for end-to-end service performance measurement in a client server environment exists. This approach, called Application Response Measurement (ARM) defines a model including an abstract definition of a unit of work and related performance records; it offers an API to application developers which allows easy integration of measurement within their distributed application. While this approach is interesting, it is only a first step toward the automation of performance management.

We are investigating two specific aspects. First we are working on the coupling and possible automation of performance measurement models with the upper service level agreement and specification levels. Second we are working on the mapping of these high level requirements to the lower level of instrumentation and actual data collection processes available in the network. More specifically we are interested in providing automated mapping of service level parameters to monitoring and measurement capabilities. We also envision automated deployment and/or activation of performance measurement sensors based on the mapped parameters. This activity also incorporates self-instrumentation (and when possible on the fly instrumentation) of software components for performance monitoring purpose.

4. Application Domains

4.1. Mobile, ad-hoc and constrained networks

The results coming out from MADYNES can be applied to any dynamic infrastructure that contributes to the delivery of value added services. While this is a potentially huge application domain, we focus on the following environments at the network level:

1. multicast services,
2. ad-hoc networks,
3. mobile devices and IPv6 networks,
4. voice over IP infrastructure.

All these selected application areas exhibit different dynamicity features. In the context of multicast services, we focus on distribution, monitoring and accounting of key distribution protocols. On *ad-hoc* and dynamic networks we are investigating the provisioning, monitoring, configuration and performance management issues.

Concerning mobile devices, we are interested in their configuration, provisioning and monitoring. IPv6 work goes on in Information Models and on self-configuration of the agents.

4.2. Dynamic services infrastructures

At the service level, dynamics is also increasing very fast. We apply the results of our work on autonomous management on infrastructures which support dynamic composition and for which self-instrumentation and management automation is required.

The target service environments are:

- sensor networks,
- peer-to-peer infrastructures,
- information centric networks,
- ambiant environments.

5. New Software and Platforms

5.1. Escape

Participants: Thibault Cholez [contact], Shbair Wazen.

Initially developed by Antoine Goichot during his internship [47], from reasearch results of Wazen Shbair, Thibault Cholez and Isabelle Chrisment.

Escape is a Firefox web browser addon designed and developed by the team to bypass some HTTPS filtering strategies. The extension was built in the context of evaluating HTTPS traffic filtering techniques based on the Server Name Indication (SNI) extension of TLS and which have been recently used by many firewalls for filtering websites accessed through HTTPS. Our tool mainly offers the ability to bypass such firewalls by editing on-the-fly the SNI field with alternate values and therefore access the blocked HTTPS websites. In addition, it can be used to bypass legacy filtering of DNS requests. The extension is implemented in JavaScript and is based on another security addon named Convergence. Escape is distributed under a GPL3 Open Source license and can be downloaded on the team website.

5.2. MPIGate

Participants: Mandar Harshe, Ye-Qiong Song [contact].

MPIGate stands for Multi Protocol Interface GATEway for Tele-care, Environment Monitoring and Control. It was initiated by TRIO Team of LORIA and Inria Nancy Grand-est, in October 2009 as a follow-up of wireless sensor network (WSN) projects in ambient assisted living, smart home, logistic and industry domains. Since 2012, its evolution is continuously ensured by members of MADYNES Team. It is a set of software aiming at facilitating the development of both home automation and ambient assisted living applications thanks to the abstraction of heterogeneous sensor data and the facility of access to read and write functions over the devices plugged to the networks (wired and wirelessly). The key features of MPIGate include the drivers for different networks protocols (Bluetooth, WiFi, IEEE802.15.4/Zigbee, KNX, EnOcean) and a ROS-based middleware layer offering modularity and quality of service. This year, its evolution has mainly been carried out within SATELOR project and IPL PAL project. It can be used by people working on home automation and ambient assisted living applications. Further information can be found at http://mpigate.loria.fr.

5.3. AA4MM

Participants: Laurent Ciarletta [contact], Yannick Presse, Benjamin Segault.

Benjamin Camus, Victorien Elvinger, Vincent Chevrier (contact), Julien Vaubourg, and Christine Bourjot from the MAIA team, LORIA are contributors for this software.

AA4MM (Agents and Artefacts for Multi-modeling and Multi-simulation) is a framework for coupling existing and heterogeneous models and simulators in order to model and simulate complex systems. The first implementation of the AA4MM meta-model was proposed in Julien Siebert's PhD [51] and written in Java, and a renewed Java version was submitted to the APP (Agence pour la protection des programmes).

We are using this software in a strategic action with EDF R&D in the context of the simulation of smart-grids in the frame of the MS4SG (Multi-Simulation fro Smart Grids) project. Julien Vaubourg started a PhD on this project that is co-directed by Laurent Ciarletta and Vincent Chevrier. The 2014 year was dedicated to improve existing software and to develop new components thanks to new scientific contributions.

Currently, two new pieces of software are being submitted to the APP:

1. a modelling environment software that enables the graphical definition of multi-models from preexisting elements.
2. AA4MM-Visu, a plug-in dedicated to the collection and visualization of information during simulation.

We plan to submit an enhanced version of the JAVA software and of the AA4MM-Visu. The core elements of AA4MM will be made available early in 2015 under an open licence.

5.4. Platforms

5.4.1. Android Security platform

Participants: Abdelkader Lahmadi [contact], Rémi Badonnel, Olivier Festor, Eric Finickel, Frederic Beck [SED, Inria Nancy Grand Est].

Android environments are facing several threats and attacks. Madynes team is working on the development of a monitoring platform dedicated to the security analysis and these environments. The monitoring platform relies on different components:

- a set of probes dedicated to the measurement of network activities using NetFlow protocol and logs generated by running Applications of an Android device. An OVAL agent (Ovaldroid) is also developed for vulnerability assessment.
- a set of scalable data collectors to collect and parse the data issued by our probes (NetFlow records, logs in the syslog format and vulnerability reports). The collectors are relying on Flume agents.
- a NoSQL storage (HBase) engine where all the collected data are stored for further analysis.
- A first set of analysers of the collected data, relying on a Map-Reduce engine (Spark) are also developed [41] including statistical analysis about connected services and ports but also a Self-Organising Map analyser to classify Android application patterns according to different properties including their communication patterns and also their lifecycle activities. [16].

The first version of the monitoring platform is operational and deployed within the LHS infrastructure. Further development is currently under taken to provide more analysis, data correlation and visualisation features.

5.4.2. IoT platform

Participants: Emmanuel Nataf [contact], Thibault Cholez.

This platform is a joint work between Anthony Deroche [43], Thierry Duhal [45] and Arthur Garnier [46], respectively students from TELECOM Nancy and IUT Nancy-Charlemagne. They worked under the supervision of Emmanuel Nataf and Thibault Cholez between February and August 2014.

The main goal of the IOT platform is to collect and store production and management data produced during long-run WSN experiments. The platform is open-source (https://github.com/AnthonyDeroche/iotlab/) and built with a modular architecture in order to support different types of experiment (routing algorithms, energy efficiency, security, etc.).

Based on this platform, we developed several innovative applications:

- indoor geolocalization of sensors based on RSSI strength [43]
- data collection from several concurrent points allowing better scalability with good performances on large WSN [45]
- data link to remotely control nodes from the web interface with a skeleton of API [45]

Regarding the technical aspects [44], the platform is based on a JEE architecture running on a Glassfish server, websocket full-duplex communications, secure and authenticated administrator access (HTTPS). The web interface uses the framework CSS front-end Zurb Foundation and javascript libraries to display dynamic charts and maps.

The full plateform has been instantiated with 40 TELOSB sensors deployed in TELECOM Nancy (http://iotlab.telecomnancy.eu/) during one month.

5.4.3. SCADA platform

Participants: Abdelkader Lahmadi [contact], Jérôme François, Olivier Festor.

SCADA is a term used in several industries and its stands for *Supervisory Control and Data Acquisitions*. It refers to a centralized control and monitoring system for a variety of machinery and equipment involved with many industrial activities. SCADA systems are also becoming target to different attacks exploiting traditional IT vulnerabilities, e.g. buffer overflows, script crossing, crafted network packets, or specific vulnerabilities related to control and estimation algorithms employed by control processes.

We are developing and maintaining a platform to assess and analyse the security of SCADA systems based on a testbed combining real hardware and simulation tools of physical processes. We have extended our SCADA testbed to simulate a microgrid scenario [49]. We are thus able to extract and analyse the Profinet messages at the control network level using process mining techniques. Further development will be taken to include information technology layers in the testbed (servers, firewalls, network devices, etc).

During the year 2014, we have also started the development of a scanning platform of Internet IP addresses and communication ports to identify exposed sensitive services and networks, for instance SCADA systems [42].

6. New Results

6.1. Highlights of the Year

The following points of 2014 deserves to be highlighted:

- One new permanent member joined the MADYNES team: Jérôme François as Inria researcher.
- An IBM Faculty Award has been received by a team member (Rémi Badonnel, TELECOM Nancy) for his work on security and cloud computing.

BEST PAPER AWARD :
[21] **A Study of RPL DODAG Version Attacks in 8th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2014**. A. MAYZAUD, A. SEHGAL, R. BADONNEL, I. CHRISMENT, J. SCHÖNWÄLDER.

6.2. Monitoring

6.2.1. P2P network monitoring

Participants: Thibault Cholez [contact], Isabelle Chrisment, Olivier Festor.

Finishing a work started several years ago with our colleagues from the team Complex Network [1] at the LIP6, we published a final result on the comparison of paedophile activity in different P2P systems [5]. We designed a methodology for comparing KAD and eDonkey, two P2P systems among the most prominent ones and with different anonymity levels. We have detected paedophile-related queries with a previously validated tool and we proposed, for the first time, a large-scale comparison of paedophile activity in two different P2P systems.

We are also glad to have contributed to a book chapter in french on the uses and misuses of digital identities on the Internet [33]. It summarizes several years of work of the team, fighting against the Sybil attack in P2P networks in order to improve their security and quality of service.

6.2.2. Anonymous networks monitoring

Participants: Juan Pablo Timpanaro, Isabelle Chrisment [contact], Olivier Festor.

Anonymous networks have emerged to protect the privacy of network users. Large scale monitoring on these systems allows us to understand how they behave and which type of data is shared among users.

In 2014, we continued our research about the I2P anonymous network [2]. This network is optimized for anonymous web hosting and anonymous file-sharing. I2P's file-sharing community is highly active with users deploying their file-sharing applications on top of the network. I2P uses a variation of Onion routing, thus assuring the unlinkability between a user and its file-sharing application. In [26] we took the first step towards the linkability of users and applications in the I2P network. We conducted a group-based characterization, where we determine to what extent a group of users is responsible for the overall I2P's file-sharing activity. We used Pearson's coefficient to correlate users from two cities and the most used anonymous file-sharing application.

6.2.3. Smartphone usage monitoring

Participants: Vassili Rivron [contact], Mohammad Irfan Khan, Simon Charneau [Inria], Isabelle Chrisment.

Over the last few years the number of smartphone applications has increased enormously. In 2014, we passively collected smartphones usage logs in the wild by inviting the crowd to participate in the PRACTIC [3] contest and install our crowdsensing application to contribute anonymous smartphone usage logs, voluntarily and in the most natural settings (their own phone, own pricing plan) .

Complementary to sensing we also collected contextual information (social, demographic, professional) and information about users'perception via survey questionnaires built in the application or on the web.

This experiment used a crowd sensing platform called APISENSE ®[4] and developed by the Inria Spirals Team. It was carried out in the context of building a country-wide Internet observation platform in France, called Metroscope [5].

6.3. Security

6.3.1. Security Automation

Participants: Rémi Badonnel [contact], Martin Barrere, Gaëtan Hurel, Abdelkader Lahmadi, Olivier Festor.

The main research challenge addressed in this work is focused on enabling configuration security automation in dynamic networks and services.

[1] http://www.complexnetworks.fr/
[2] http://i2p2.de
[3] http://beta.apisense.fr/practic
[4] http:///www.apisense.com/
[5] http://metroscope.eu/

A first part of our work in the year 2014 was centered on a strategy for remediating known vulnerabilities, formalizing the correction decision problem as a satisfiability or SAT problem [10]. From a proactive perspective, it should be able to decide which potential states could be dangerous. By specifying our vulnerability knowledge source (OVAL repository) as a propositional logical formula, we have fixed system properties that we cannot change and free those variables for which changes are available. We have introduced the X2CCDF language, built on top of XCCDF and OVAL, that allows us to express the impact of these changes over target systems. These descriptions can be used for analyzing the security impact of changes without actually changing the system. When this information is not available, we have considered the NETCONF protocol and its notion of candidate state where changes can be applied, analyzed and rolled back if necessary.

A second part of our work has been dedicated to the orchestration of security functions in the context of mobile smart environments [19]. Most of current security approaches for these environments are provided in the form of applications or packages to be directly installed on the devices themselves inducing local resource consumption. In that context, we have investigated a new approach for outsourcing mobile security functions as cloud-based services for smartphones and tablets [32]. The outsourced functions are dynamically activated, configured and orchestrated using software-defined networking and virtualization techniques. We consider the use of security compositions in order to dynamically fit the security requirements of mobile devices according to their current contexts. This approach is based on different traversal schemes (sequential, conditional, and concurrent). The solution has been prototyped based on the mininet software-defined networking emulator, jointly with mobile devices using the android operating system.

6.3.2. SDN-based security

Participants: Jérôme François [contact], Lautaro Dolberg [University of Luxembourg], Olivier Festor, Thomas Engel [University of Luxembourg].

By decoupling the data and control plane, Software-Defined Networking allows a fine grained network management. Protocols like OpenFlow allow multiple actions like traffic forwarding or blocking but also modifications or monitoring with the extensive use of counters. Hence, many approaches have emerged the last year to enable some security functions like firewalls, flow monitoring and traffic redirection to middleboxes. These different scenarios have been evaluated in a survey paper [17] in cooperation with the university of Luxembourg.

Furthermore, we also proposed to leverage SDN, especially OpenFlow, for forensics purpose [18]. Indeed, through a recursive analysis on network path and flow tables in OpenFlow, it is possible to reconstruct the paths traversing by an anomaly.

6.3.3. Phishing Detection

Participants: Jérôme François [contact], Samuel Marchal [University of Luxembourg], Radu State [University of Luxembourg], Thomas Engel [University of Luxembourg].

This work is a joint work with the University of Luxembourg.

The language used for phishing is a particular language aiming at attracting victims. To achieve that the attackers uses specific words related to well known brand names and reassuring words. Our method to detect such abnormal domain names relies on word decomposition and semantic analysis. As an example, we can learn if having both *microsoft* and *protected* in domain is significative of a malicious domain. Actually, not all words can be represented during the learning and we use semantic similarities to also extend this knowledge (for example, we can *derive* safe from *protected*).

Our recent work [20] was focusing on extending this domain-based analysis to the full analysis of an url. We have also observed that most of false positives or negatives we obtained with previous methods are biased by natural language corpus while the *Internet vocabulary* is different.

Hence, we extracted from Google and Yahoo statistics about search queries. Our observation highlights that the relation between the different parts of the URL (the domain and the path) is a discriminative feature for malicious URL identification.

Finally, a more in-depth feature analysis is provided in [8], which also proposes leveraging streaming data analytics by instantiating our method on Storm.

6.3.4. Flows and logs analysis

Participants: Jérôme François [contact], Abdelkader Lahmadi.

Machine generated-log data is a fundamental part of information technology systems. They are usually generated at every component of distributed information systems including routers, security products, web proxies, DHCP servers, VPN servers, or any end-points like mobile devices or connected things, etc. They often contain high volumes of interesting information and are among the first data source to be analyzed for the detection of abnormal activities due to running attacks or malicious running applications. A better understanding of these attacks and malicious applications requires the elaboration of efficient and novel methods and techniques able to analyze these logs.

In [16], we carried an empirical analysis of the logs generated by the logging system available in Android environments. The logs are mainly related to the execution of the different components of applications and services running on an Android device. We have analyzed the logs using self organizing maps where our goal is to establish behavioral fingerprints of Android applications. The developed methodology allows us the better understand Android Apps regarding their granted permissions and performed actions.

During the year 2014, we have also maintained an IETF draft [50] to make a standardization effort towards the extension of IP Flow-based monitoring with geographic information. Associating Flow information with their measurement geographic locations will enable security applications to detect anomalous activities. In the case of mobile devices, the characterization of communication patterns using only time and volume is not enough to detect unusual location-related communication patterns.

6.3.5. Sensor networks monitoring

Participants: Rémi Badonnel, Isabelle Chrisment, Olivier Festor, Abdelkader Lahmadi [contact], Anthéa Mayzaud.

Low Power and Lossy Networks (LLNs) are made of interconnected wireless devices with limited resources in terms of energy, computing and communication. The communication channels are low-bandwidth, high loss rate and volatile wireless links subject to failure over time.

This year, our work on security-oriented monitoring [28] has focused on quantifying the effects of version number manipulation attacks within RPL networks [21]. Through simulations it was discovered that control overhead can increase by up to 18 times, thereby impacting energy consumption and channel availability. This in turn can reduce the delivery ratio of packets by up to 30% and nearly double the end-to-end delay in a network. A strong correlation between the position of the attacker and the effect on the network was also observed.

In that context, we have designed a mitigation strategy based on an adaptive threshold to cover a large variety of DODAG inconsistency attacks [25] in a lightweight manner. Currently RPL attempts to counteract such attacks by using a fixed threshold. During experimentations it becomes clear that the adaptive threshold is able to reduce the control message overhead, compared to fixed threshold, by up to 13% in short lived and 55% in long-lived networks. This leads to large reductions, i.e., between 10%-40%, in energy consumption.

In addition, we have investigated a distributed passive monitoring architecture for RPL-based advanced measurement infrastructure networks.

6.3.6. Intrusion Detection System in Wireless Sensor

Participants: Emmanuel Nataf [contact], Hubert Kenfack Ngankam.

This work is based on a previous work about the definition of an ontology to classify intrusion attacks in a wireless sensors network. A first implementation of this ontology focuses on the black hole and the sink hole intrusion where some malicious sensor node either do not forward data to a central point of collect or try to be elected as the best next hop toward the central point.

We look at discover malicious nodes by an analysis of the network topology obtained by data gathered from the network itself. At regular interval, we built a snapshot view of the network topology and compare it with the previous one in order to detect anomalies such as a whole sub network that disappear or an under-optimal network topology.

Simulation results are good and we will continue on this way.

6.3.7. SCADA systems security

Participants: Abdelkader Lahmadi [contact], Younes Abid.

SCADA systems are facing several attacks and threats which are growing in number and complexity. A key challenge in this context is the simulation and the assessment of the impact and the propagation of these attacks on SCADA system components over time. During the year 2014, we have developed a novel methodology [38] based on stochastic modeling to simulate the impact of attacks on SCADA systems. The system is modeled as a network of interacting markov chains and the impact of an attack is simulated using the influence model. In this model, the state of each node of the system is either influence by its own Markov chain or by the state of its neighboring nodes. We have modeled and analyzed a SCADA system with 200 control nodes and several servers. We have modeled different attacks (intrusion, DoS, malware) where attack nodes are introduced in the interacting SCADA network to influence control node behaviors. For each attack, we have simulated and assessed over time the availability of the overall system regarding the number of failed nodes.

6.3.8. Management of HTTPS traffic

Participants: Thibault Cholez [contact], Isabelle Chrisment, Shbair Wazen, Jérôme François.

Surveys show that websites are more and more being served over HTTPS. They highlight an increase of 48% of sites using TLS over the past year (2013),

We investigated the latest technique for HTTPS traffic filtering that is based on the Server Name Indication (SNI) field of TLS and which has been recently implemented in many firewall solutions. We show that SNI has two weaknesses, regarding (1) backward compatibility and (2) multiple services using a single certificate. We demonstrated thanks to a web browser plug-in called *Escape* that we designed and implemented, how these weaknesses can be practically used to bypass firewalls and monitoring systems relying on SNI. The results show positive evaluation (firewall's rules successfully bypassed) for all tested websites. This work will be published in the experience session of the IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM'15).

We also started a new work on the precise identification of websites accessed through HTTPS in the context of network forensic investigation. We use a new set of features in conjunction with machine learning techniques to achieve a high accuracy.

6.4. Routing

6.4.1. Routing in Wireless Sensor Networks

Participants: Emmanuel Nataf [contact], Patrick-Olivier Kamgueu.

We deployed a wireless sensors network in the laboratory during two time period of 3 months. The first was with the legacy routing (based on expected transmission time metric) and the second was with our routing process based on a composition of several metrics (i.e. energy, transmission time and delay) by the use of fuzzy logic. We have compared these experiments by packet loss ratio and energy consumption. In all case, our routing leads to a better network [48].

6.4.2. Operator calculus based routing in Wireless Sensor Networks

Participants: Evangelia Tsiontsiou, Bernardetta Addis, Ye-Qiong Song [contact].

For supporting different QoS requirements, routing in WSN must simultaneously consider several criteria (e.g., minimizing energy consumption, hop counts or delay, packet loss probability, etc.). When multiple routing metrics are considered, the problem becomes a multi-constrained optimal path problem (MCOP), which is known as NP-complete.

Recently, Operator calculus (OC) has been developed by Schott and Staples with whom we collaborate. We make use of OC methods on graphs to solve path selection in the presence of multiple constraints. Based on OC, we developed a distributed algorithm for path selection in a graph. We also designed a new routing protocol which makes use of this algorithm: the Operator Calculus based Routing Protocol (OCRP). In OCRP, a node selects the set of eligible next hops based on the given constraints and the distance to the destination. It then sends the packet to all eligible next hops. The protocol is implemented in Contiki OS and emulated for TelosB motes using Cooja. We compared its performance against tree and directional flooding routing and show the advantages of our technique. Our ongoing work consists in its comparison with RPL to show its effective contribution to handle simultaneously several IETF ROLL routing metrics.

This work is under development as part of Lorraine AME Satelor project.

6.4.3. *Energy-aware IP networks management*

Participants: Bernardetta Addis [contact], Giuliana Carello [DEIB, Politecnico di Milano, Italy], Antonio Capone [DEIB, Politecnico di Milano, Italy], Luca Gianoli [Polytecnique de Montreal, Canada], Sara Mattia [IASI, CNR, Roma, Italy], Brunide Sansò [Polytecnique de Montreal, Canada].

The focus of our research is to minimize the energy consumption of the network through a management strategy that selectively switches off devices according to the traffic level. We consider a set of traffic scenarios and jointly optimize their energy consumption assuming a per-flow routing. We propose a traffic engineering mathematical programming formulation based on integer linear programming that includes constraints on the changes of the device states and routing paths to limit the impact on quality of service and the signaling overhead. We also present heuristic results to compare the optimal operational planning with online energy management operation ([3])

Two very important issues that may be affected by green networking techniques are resilience to node and link failures, and robustness to traffic variations. We thus extended the optimization models. To guarantee network survivability we consider two different schemes, dedicated and shared protection, which assign a backup path to each traffic demand and some spare capacity on the links along the path. Robustness to traffic variations is provided by tuning the capacity margin on active links in order to accommodate load variations of different magnitude. Both exact and heuristic methods are proposed. Experimentations carried out on realistic networks operated with flow-based routing protocols (like MPLS) allow us to quantitatively analyze the trade-off between energy cost and level of protection and robustness. Results show that significant savings, up to 30%, may be achieved even when both survivability and robustness are fully guaranteed [4].

Computational cost of proposed models can be very high when dealing with large size instances (network size and/or number of demands). For this reason, we proposed and tested different problem formulations with the aim of solving larger size instances at optimality. Preliminary results on a simplified model ([29]) are very encouraging.

6.4.4. *Energy-aware joint management of networks and Cloud infrastructures*

Participants: Bernardetta Addis [contact], Danilo Ardagna [DEIB, Politecnico di Milano, Italy], Giuliana Carello [DEIB, Politecnico di Milano, Italy], Antonio Capone [DEIB, Politecnico di Milano, Italy].

Fueled by the massive adoption of Cloud services, overall service centers and networks account for 2–4% of global CO_2 emissions and it is expected they can reach up to 10% in 5–10 years.

The geographical distribution of the computing facilities offers many opportunities for optimizing energy consumption and costs by means of a clever distribution of the computational workload exploiting different availability of renewable energy sources, but also different time zones and hourly energy pricing. Energy and cost savings can be pursued by dynamically allocating computing resources to applications at a global

level, while communication networks allow to assign flexibly load requests and to move data. We propose an optimization framework able to jointly manage the use of brown and green energy in an integrated system and to guarantee quality requirements. We propose an efficient and accurate problem formulation that can be solved for real-size instances in few minutes to optimality. Numerical results, on a set of randomly generated instances and a case study representative of a large Cloud provider, show that the availability of green energy have a big impact on optimal energy management policies and that the contribution of the network is far from being negligible ([2]).

6.4.5. Content centric wireless sensor networks

Participants: Abdelkader Lahmadi [contact], Younes Abid, Olivier Festor.

During this year, we have instantiated a novel named data aggregation method [9] dedicated to wireless sensor networks . The method relies on an adaptation of the CCNx protocol implementation that we have developed in a previous work. Our method extends the CCNx protocol with in-network processing functions to aggregate named data efficiently. We have implemented and tested our solution with the Contiki operating system which is an operating system for resources-constrained embedded systems and wireless sensor networks. Our simulation and measurement results using the Cooja simulator and physical nodes show that our solution has a small overhead in terms of exchanged messages and provides acceptable data retrieval delays.

6.5. Quality-of-Service

6.5.1. ICN cache management

Participants: Olivier Festor [contact], César Bernardini, Thomas Silverston.

Information Centric Networking (ICN) has become a promising new paradigm for the future Internet architecture. It is based on named data, where content address, content retrieval and the content identification is led by its name instead of its physical location. One of the ICN key concepts relies on in-network caching to store multiple copies of data in the network and serve future requests, which helps reducing the load on servers, congestion in the network and enhances end-users delivery performances. As a central component of ICN is in-network caching, the ely used as a micro-blogging service. At the same time, Online Social Networks (OSN) carry extremely valuable information about users and their relationships. We argue that this knowledge can help to drastically improve the efficiency of ICN.

We therefore propose SACS, a caching strategy designed for the CCN architecture that includes social information [11]. CCN is to date the most widely adopted ICN architecture by the research and industrial community. The underlying idea in such strategy is that a small number of users counts a huge amount of social relationships, dominates the activity and receives most attention from other users. We call such users Influential users, and we argue that they produce content that is more likely to be consumed by others, and in consequence their content must be favored and replicated in priority. Our novel caching strategy is therefore prioritizing content from Influential users of the social network. To validate our strategy, we first propose a model of social network over the CCN architecture [30]. Our model has been designed based on the measurement of Pinterest, a web-based OSN system. Extensive simulations of the strategy have been performed, as well as a real implementation on CCNx and deployment over the PlanetLab testbed. Our results with SACS are significant and increase drastically the caching performance of ICN architecture. content

Efficient management of caches is a key success factor in Concent-Centric Networks where multiple (up to every single node in the network) entities act as caches of the shared content in the network. We pursued our investigations towards a common evaluation framework for cache strategies in Content-centric networks and towards the definition of novel cache strategies, exploiting context information available at the service level of today's internet.

6.5.2. Self-adaptive MAC protocol for both QoS and energy efficiency

Participants: Kévin Roussel, Shuguo Zhuo, Ye-Qiong Song [contact].

WSN research focus has progressively been moved from the energy issue to the QoS issue. Typical example is the MAC protocol design, which cares about not only low duty-cycle at light traffic, but also high throughput with self-adaptation to dynamic traffic bursts.

The two MAC protocols that we have previously designed namely S-CoSenS and iQueue-MAC, have been successfully implemented on SMT32W108 SoC chips. Two contributions have been made this year. Firstly iQueue-MAC has been extended to work on both single channel mode and multi-channel mode, improving its throughput performance. Secondly, both S-CoSenS and iQueue-MAC have been implemented on RIOT OS. An additional contribution is related to the RIOT OS development itself since we have improved the robustness of the existing ports of RIOT OS on MSP430-based motes, making it a suitable software platform for tiny motes and devices. More generally, through this part of work, we have shown that RIOT OS is also suitable for implementing high-performance MAC protocols, thanks to its real-time features (especially hardware timers management). Part of this work has been supported by ANR-NFSC Quasimodo and PIA LAR projects.

6.5.3. *End-to-end delay modelling and evaluation in wireless sensor networks*

Participants: François Despaux, Abdelkader Lahmadi, Ye-Qiong Song [contact].

Probabilistic end-to-end performance guarantee may be required when dealing with real-time applications. As part of ANR QUASIMODO project, we are dealing with Markov modeling of multi-hop networks running duty-cycled MAC protocols. One of the problems of the existing Markovian models resides in their strong assumptions that may not be directly used to assess the end-to-end delay in practice. In particular, realistic radio channel, capture effect and OS-related implementation factors are not taken into account. We proposed to explore a new approach combining code instrumentation and Markov chain analysis. In [15] we have presented a new approach for extracting empirical Markov chain models from network protocol traces by means of Process Mining techniques. An empirical Markov chain model was obtained for the IEEE 802.15.4 beacon-enabled mode protocol allowing us to estimate the e2e delay for a multi-hop scenario. This approach has also been successfully applied to the case of ContikiMAC [14].

6.5.4. *Dynamic resource allocation in network virtualization*

Participants: Mohamed Said Seddiki, Mounir Frikha [SupCom, Tunis, Tunisie], Ye-Qiong Song [contact].

The objective of this research topic is to develop different resource allocation mechanisms in Network Virtualization, for creating multiple virtual networks (VNs) from a single physical network. It is accomplished by logical segmentation of the network nodes and their physical links.

This year we have focused on implementing and evaluating the used of SDN for managing the QoS in broadband access networks. Unfortunately, application-based QoS on a home network gateway faces significant constraints, as commodity home routers are not typically powerful enough to perform application classification, and many home users are not savvy enough to configure QoS parameters. In [24] we designed FlowQoS, an SDN-based approach where users can specify upstream and downstream bandwidth allocations for different applications at a high level, offloading application identification to an SDN controller that dynamically installs traffic shaping rules for application flows We designed a custom DNS-based classifier to identify different applications that run over common web ports; a second classifier performs lightweight packet inspection to classify non-HTTP traffic flows. We implemented FlowQoS on OpenWrt and demonstrated that it can improve the performance of both adaptive video streaming and VoIP in the presence of active competing traffic.

This work has been carried out as part of a co-supervised PhD thesis between University of Lorraine and SupCom Tunis.

6.5.5. *Task and message scheduling in distributed real-time systems*

Participants: Florian Greff, Laurent Ciarletta, Ye-Qiong Song [contact].

QoS must be guaranteed when dealing with real-time distributed systems interconnected by a network. Not only task schedulability in processors, but also message schedulability in networks should be analysed for validating the system design. In [37], [36], [34], and [35], we provided an overview of both message scheduling techniques in networks and joint task and message scheduling approaches in closed-loop distributed control systems (networked control systems). Fault-tolerance is another critical issue that one must take into account. In collaboration with an industrial partner, we started a study on the real-time dependability of UAV multi-criticity system interconnected by an embedded mesh network. The future work aims at developing a robust mesh network routing protocol and studying the schedulability under constraints of multi-criticality and graceful degradation during mode change.

6.6. Multi-modeling and co-simulation tools for the evaluation and development of Smart* and other Pervasive Computing systems

Participants: Laurent Ciarletta [contact], Olivier Festor, Ye-Qiong Song, Yannick Presse, Emmanuel Nataf, Benjamin Segault.

Vincent Chevrier (Maia team, LORIA) is a collaborator and the correspondant for the MS4SG project, Benjamin Camus, Victorien Elvinger and Christine Bourjot (Maia team, LORIA) are collaborators for the AA4MM. Julien Vaubourg's PhD is under the co-direction of V. Chevrier and L. Ciarletta.

In Pervasive or Ubiquitous Computing, a growing number of communicating/computing devices are collaborating to provide users with enhanced and ubiquitous services in a seamless way.

These systems, embedded in the fabric of our daily lives, are complex: numerous interconnected and heterogeneous entities are exhibiting a global behavior impossible to forecast by merely observing individual properties. Firstly, users physical interactions and behaviors have to be considered. They are influenced and influence the environment. Secondly, the potential multiplicity and heterogeneity of devices, services, communication protocols, and the constant mobility and reorganization also need to be addressed. Our research on this field is going towards both closing the loop between humans and systems, physical and computing systems, and taming the complexity, using multi-modeling (to combine the best of each domain specific model) and co-simulation (to design, develop and evaluate) as part of a global conceptual and practical toolbox.

We proposed the AA4MM meta-model [51] that solves the core challenges of multimodeling and simulation coupling in an homogeneous perspective. In AA4MM, we chose a multi-agent point of view: a multi-model is a society of models; each model corresponds to an agent and coupling relationships correspond to interaction between agents. In the MS4SG projet which involves MAIA, Madynes and EDF R&D on smart-grid simulation, we developed a proof of concepts for a smart-appartment case[12].

In 2014 we worked on the following research topics:

- Assessment and evaluation of complex systems.

  This work, centered on the problem of controlling complex systems proposed a control architecture within Tomas Navarrete's work [22], [23]. This "equation-free" approach uses a multi-agent model to evaluate the global impact of local control actions before applying the most pertinent set of actions. Based on a partial perception of the system state, we determine which actions to execute in order to avoid or favor certain global states of the system.

  Associated to our architecture, an experimental platform has been developed to confront the basic ideas or the architecture within the context of simulated "free-riding" phenomenon in peer to peer file exchange networks. We have demonstrated that our approach allows us to drive the system to a state where most peers share files, despite given initial conditions that are supposed to drive the system to a state where no peer shares.

- Cyber Physical Systems [13]

We have led the design and implementation of the Aetournos platform at Loria. The collective movements of a flock of flying communicating robots / UAVs, evolving in potentially perturbed environment constitute a good example of a Cyber Physical System. Applying co-simulation technique we plan to develop a hybrid "network-aware flocking behavior" / "behavior aware routing protocol".

We have provided a working set of tools: multi-simulation behavior / network / physics and generic software development using ROS (Robot Operating System). The UAVs carry a set of sensor for location awareness, their own computing capabilities and several wireless networks.

The effort put in the UAVs gathers academic and research ressources from the Aetournos platform, the R2D2 ADT and the 6PO project, while applied, industrial and more R&D projects have been pursued this year (Outback Joe Search and Rescue Challenge, Alerion, Hydradrone) .

- MS4SG has given us the opportunity to link multi-simulations tools such as HLA (High Level Architecture) and FMI (Functional Mockup Interface) thanks to our AA4MM framework. We have so far successfully applied our solution to the simulation of smart apartment complex and to combine the electrical and networking part of a Smart Grid[12].

In 2015, we will continue working on the hybrid protocols and on the UAV platform, and apply our co-simulation work to Smart Grids and other Smart*.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

7.1.1. Inria-EDF Strategic action MS4SG

Participants: Yannick Presse, Benjamin Segault, Laurent Ciarletta [contact].

Vincent Chevrier (Maia team, LORIA) is a collaborator and correspondant for the MS4SG project. Benjamin Camus, Victorien Elvinger (Maia team, LORIA) are extrenal collaborators.

The MS4SG (multi-simulation for smart grids) project is granted as a strategic action between Inria and EDF. It is a joint work between the Madynes and MAIA teams from Inria-NGE and EDF R&D. The aim of the project is to provide primitives based on AA4MM in order to enable the multi-modeling and the multi-simulation of smart-grids. They can be seen as a combination of at least 3 layers: the power grid, the network used to collect information and control the system and an Information System. As these domains can influence each other, smart-grids can be considered as a kind of complex system and we are faced with multi-modeling and multi-simulation issues. Models in these simulators (and therefore simulators) are heterogeneous (at least equation based and event based models).

The idea behind MS4SG is to use simulation to help develop and evaluate future smart grids architectures, novel supervision techniques and to eventually control these systems. Instead of building a “super simulator”, our approach is stemming from our AA4MM work, and consists in integrating simulators (and models) coming from at least the three aforementioned initial different domains: electrical networks, communication networks and information systems.

7.1.2. Alerion, project

Participants: Laurent Ciarletta, Maxence Ho, Yael Kolasa, Martin Thiriau, Emmanuel Nataf [contact].

Alerion is an e-falconry startup created by a member of Madynes. Its goal is to provide novel solutions and services “for, using and eventually against" UxV (Unmanned Air ... Vehicle). The concept is to enhance existing system and design new ones by combining well designed components seen as Cyber Physical bricks.

As part of its national grant by the "Concours national d'aide à la création d'entreprises de technologies innovantes" (for the emerging category in 2013), Alerion is funding a Proof of Concept project to help in developing and validating the requirements of a couple of basic components related to functionalities such as safety mechanisms and sensor data collection.

Alerion has also actively supported the UAV Challenge team that participated to the "Outback Joe Challenge".

.

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. Satelor AME Lorraine regional project

Participants: Mandar Harshe, Bernardetta Addis, Evangelia Tsiontsiou, Ye-Qiong Song [contact].

MADYNES is involved in Satelor, a regional research and development project funded by the AME (Agence de Mobilisation Economique) of Lorraine (October 2013 – September 2016). The consortium includes academic (Univ. of Lorraine, Inria), medical (OHS) and industrial (Diatelic-Pharmagest, ACS, Kapelse, Salendra, Neolinks) partners. It aims at developing innovative and easily deployable ambient assisted living solutions for their effective use in the tele-homecare systems. Madynes team is mainly involved in the data collection system development based on wireless sensors networks and IoT technology. The first topic consists in defining the basic functions of the future SATEBOX – a gateway box for interconnecting in-home sensors to the medical datacenter, based on our previously developed MPIGate software. A first specification for achieving a beta-version prototype of the future Satebox gateway has been made. It is intentionally limited to only using Zigbee wireless sensors for providing a low-cost and easily deployable solution for the daily activity monitoring. Its first real-world deployment at a OHS hospital room has also bee carried out.Through this deployment, a lot of important lessons have been learn that enable us to improve the reliability, robustness and the accuracy of our system. The second topic is related to improving the data transfer reliability while still keeping minimum energy consumption. This has led us to focus on the multi-hop mesh network topology with multi-constrained QoS routing problem (PhD thesis of Evangelia Tsiontsiou). A state of the art study has shown the need to look for new routing algorithms and the interest of the newly developed operator calculus approach.

8.1.2. Hydradrone R&D Lorraine UL project

Participants: Adrien Guenard, Laurent Ciarletta [contact].

Funded by the Region Lorraine under the R&D program.

The Madynes team has been working on the Hydradrone project since July 2014. It is starting as a collaborative R&D regional research and development project, funded by Region Lorraine. This project is a joint work between Madynes and PEMA (Pedon Environnement et Milieux aquatiques), an SME/VSE (small and medium size Entreprise, PEM/TPE). The company is providing the use cases and terrain (and business) validation.

It consists in developing a new solution for the surveillance of aquatic environment, the Hydradrone :

- based on an hybrid UxV (Unmanned Air, Surface, Ground Vehicle),
- some Cyber Physical bricks in coherence with the Alerion concept
- and an integration in the Information System of the company

The first year is dedicated to the development of a couple hydradrone proofs of concept (the UxV) for both hardware and software (embedded / remote) and for the sensor payload "cyber physical" bricks.

The Alerion spinoff will join the consortium upon creation.

8.1.3. 6PO Research Region Lorraine and UL project

Participants: Emmanuel Nataf, Ye-Qiong Song, Yael Kolasa, Laurent Ciarletta [contact].

Funded by Region Lorraine and Université de Lorraine since 2013. Vincent Chevrier is the point of contact for the dep. 5 at Loria. Adel Belkadi (CRAN & LORIA) is co-directed by L. Ciarletta and Didier Theilliol (CRAN correspondant).

6PO ("Systèmes Cyber-Physiques et Commande Coopérative Sûre de Fonctionnement pour une Flotte de Véhicules sans Pilote") is a joint research project between the Loria and CRAN laboratories. It aims at researching solutions for safe formation flying of collaborative UAVs seen as part of a collection of Cyber Physical Systems. This led to a common publication and the organisation of a workshop in 09/2014. It is reinforced by a PhD grant from the Federation Charles Hermite that started in october 2014. Efforts will be pursued in 2015.

The project provides common use cases and scientific challenges that serve as catalysts for collaboration between teams from different research topics :

- Cyber Physical Systems, Real Time, Quality of service, Performance and Energy in Wireless Sensors and Activator Networks
- Collaborative, communicating autonomous systems and Unmanned Vehicles
- Safety, Dependabilty, Reliability, Diagnosis, Fault-Tolerance

8.2. National Initiatives

8.2.1. Quasimodo

Participants: François Despaux, Abdelkader Lahmadi, Ye-Qiong Song [contact].

The QUASIMODO ANR Blanc international project (http://quasimodo.loria.fr/) is a fundamental research project coordinated by Prof. Ye-Qiong SONG at LORIA - University of Lorraine in France and by Prof. Youxian SUN at SKLICT of Zhejiang University in China. The project started on March 2011 and will be completed at the end of 2014. It is funded by ANR grant (ANR 2010 INTB 0206 01) and NSFC grant (NSFC 61061130563). The main objective of the project is to specify, develop and evaluate algorithms and mechanisms to provide the self-adaptive QoS support for real-time applications using wireless sensor networks (WSN). This year, the iQueue-MAC has been extended (see section 6.5.2) and we presented a method to estimate the e2e delay for a multi-hop scenario (section 6.5.2)

8.2.2. ANR Doctor

Participants: Thomas Silverston [contact], Thibault Cholez [contact], Elian Aubry, Jérôme François, Abdelkader Lahmadi, Olivier Festor.

The DOCTOR project is an applied research project funded by the French National Research Agency (ANR), grant <ANR-14-CE28-000>, and supported by the french Systematic cluster. The project officially started on October 2014 with a effective beginning of the scientific work on December 2014. It involves five partners specialized in network architectures, network monitoring and network security: three industrial partners (Orange Labs, Thales and Montimage) and two academic partners (Université de technologie de Troyes, LORIA).

Information-Centric Networking (ICN), a novel promising networking paradigm that allows adapting networks to current content-centric usage patterns, raises many deployment issues. The DOCTOR project advocates the use of virtualized network equipment (Network Functions Virtualization), enabling the co-existence of such IP and ICN stacks and the progressive migration of traffic from one stack to the other while guaranteeing the good security and manageability of the network that are primary operator requirements that need to be assured before deploying new solutions. Therefore in DOCTOR, the main goals of the project are: (1) the efficient deployment of emerging networks functions or protocols in a virtualized networking environment; (2) the monitoring and security of virtually deployed networking architectures.

This year, we mainly prepared the kickoff meeting that took place the 10th of December in Orange Labs, Issy-les-Moulineaux. We also started a joint work with UTT to write a survey on Named-Data Networking with an emphasis on the deployment and security questions.

8.2.3. ANR LAR

Participants: Kévin Roussel, Ye-Qiong Song [contact].

LAR (Living Assistant Robot) is a national project getting together Inria (MAIA and MADYNES teams), Credit Agricole, Diatelic and Robotsoft. The aim is to develop an ambient assisted living system for elderly including both sensors and assistant robots. The task of our team is the development of a WSN based system integrating both sensors of the environment and sensors and actuators embedded on a mobile robot. The research issues include the QoS, energy and mobility management. This year we identified RIOT OS as our software platform for developing both protocols and IoT applications. We also evaluated and fixed three hardware platforms (Zolertia MSP430 Z1, AVR ATmega256RFR2 and Arduino DUE) for the development of the project. We have improved the robustness of the existing ports of RIOT OS on MSP430-based motes. Two MAC protocols (S-CoSenS and iQueue-MAC) have been implemented on RIOT-OS (see section 6.5.2).

8.2.4. PEPS Humain - CNRS Project TrustSourcing

Participants: Thomas Silverston [contact], Vassili Rivron, Isabelle Chrisment.

Crowdsourcing relies on the participation of users collecting information in order to perform complex tasks. The participating users and the collected data should be of high quality for offering a trustable service to all the users. In the Trustsourcing project, we propose to design a Trust mechanism adapted to the crowdsourcing paradigm. Based on the current work initiated by the Metroscope/PRACTIC initiative, whose main goal is to study the usage of smartphone by measuring users' activity, we will propose to classify smartphone users and deduce some categories of trustable users. According to their "fingerprint" usage of their smartphone (time spent with phone, number of applications, messages etc.), we could estimate if an user will more probably belong to a category of trustable users or not. Our predictive mechanism will rely on the measurement of realistic users' activity and could help limiting drastically the impact of malicious users and the deterioration of the crowdsourcing service.

8.2.5. Action de Développement Technologique

8.2.5.1. ADT Métroscope

This ADT is linked to the consortium Metroscope [6], whose goal is to understand the behavior of the Internet and its uses within a mobile environment. Through this ADT, funded by Inria, an engineer (Mohammad-Irfan Khan) was hired for 2 years (2013-2015). He is participating in the design and deployment of a distributed platform. This platform is composed of a services providing measurement tools that collect a set of data and interact with probes located at various points of the network.

8.2.5.2. ADT SEA

The goal of this ADT is to provide an novel security solution for Android platforms where the users will be able to evaluate the security level of their devices. The solution relies on the analysis and collection of logs and network activities of running Android applications to detect malicious activities and also the detection of vulnerable configurations of the device using an OVAL-based approach. Through, this ADT, funded by Inria, an engineer (Eric Finickel) was hired for 2 years (2013-2015). He is working on the development of Android devices embedded probes to export logs and network activities. He will also design and setup the collector and the analysis applications using a Hadoop based framework. It is currently deployed in the High Security Lab.

8.2.5.3. ADT R2D2

The goal of this ADT is to provide assistance in developing the Aetournos platform. Through this ADT, funded by Inria, an engineer (Ceilidh Hoffmann) was hired for the year (2014). She has been helping maintaining the Aetournos platform, coordinating students work on the platform and tutoring the Aetournos team for the Outback Joe Search and Rescue Challenge. She is also developing tools for UAV localization using visual cues.

[6] http://metroscope.eu/

8.2.6. Inria Project Lab PAL

The Inria Large-scale initiative action IPL PAL project (http://pal.inria.fr) aims at providing technologies and services for improving the autonomy and quality of life for elderly and fragile persons. Communication is one of the key components for ensuring real-time data gathering and exchange between heterogeneous sensors and actuators (robots). Within PAL project and using LORIA's smart apartment platform (http://infositu.loria.fr), we extended MPIGate (http://mpigate.loria.fr) functionalities by adding EnOcean sensors and defining a unified data format in JSON to ease the exchange with other data servers. The adoption of ROS (Robotic Operating System) as middleware also facilitates the interoperability of our services with the services of the other PAL partners since the new PALGate is based on ROS.

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

8.3.1.1. FI-WARE

Type: COOPERATION Future Internet Core Platform

Instrument: Integrated Project

Objective/Topic: PPP FI - Technology Foundation: Future Internet Core Platform

Duration: September 2011 - May 2014

Coordinator: Telefonica (Spain)

Partners: Thales, SAP, Inria

Inria contact: Olivier Festor

See also: http://www.fi-ware.eu

Abstract: FI-WARE will deliver a novel service infrastructure, building upon elements (called Generic Enablers) which offer reusable and commonly shared functions making it easier to develop Future Internet Applications in multiple sectors. This infrastructure will bring significant and quantifiable improvements in the performance, reliability and production costs linked to Internet Applications, building a true foundation for the Future Internet.

The goal of the FI-WARE project is to advance the global competitiveness of the EU economy by introducing an innovative infrastructure for cost-effective creation and delivery of services, providing high QoS and security guarantees. The key deliverables of FI-WARE will be an open architecture and a reference implementation of a novel service infrastructure, building upon generic and reusable building blocks developed earlier.

The MADYNES contributions to the FI-WARE project are:

- Sicslowfuzzer, a fuzzing framework for the Internet of Things, that allows to assess the robustness of IoT OSes and applications, networkwise.
- Flowoid, a netflow probe for Android-based devices, which also provides a netflow location template to convey location information of the device;
- XOvaldi4Android, an OVAL interpreter for Android-based devices, that is able to retrieve OVAL definitions using a web service, use them to check the current status of the system, and publish a result, using a second web service;
- the coordination between the Security Work Package and the Inria teams involved in it. This includes the attending to weekly audio conferences, face to face meetings, and making sure deliverables and tasks were addressed in a timely manner.

During 2014, all the contributions of the Madynes team including the developed tools and their respective documentation have been delivered and validated by the Work Package leader.

8.3.1.2. Flamingo

Type: FP7

Instrument: Network of Excellence

Objective/Topic: Management of the Future Internet

Duration: November 2012 - October 2016

Coordinator: University of Twente (Netherlands)

Partners: University of Twente, Inria, University of Zurich, Jacobs University of Bremen, University des Bundeswehr Munich, Polytechnic University of Catalonia, Interdisciplinary Institute for Broadband Technology, University of Ghent, University College London

Inria contact: Olivier Festor

See also: http://www.fp7-flamingo.eu

Abstract: The FP7 FLAMINGO Network of Excellence is composed of 8 partner universities, with complementary knowledge and strong ties to industry. It covers the entire spectrum of network management core functions and application domains, which are required for building, integrating, and disseminating the knowledge of the management plane for the Future Internet.

The objectives of FLAMINGO are (a) to strongly integrate the research of leading European research groups in the area of network and service management, (b) to strengthen the European and worldwide research in this area, and (c) to bridge the gap between scientific research and industrial application. To achieve these goals, FLAMINGO performs a broad range of activities, such as to develop open source software, establish joint labs, exchange researchers, jointly supervise Ph.D. students, develop educational and training material, interact with academia and industry, organize event, and strongly contribute to (IETF and IRTF) standardization.

Our work on network and service monitoring has focused on security for mobile and low power networks. We have proposed a strategy for addressing DODAG-based attacks [25], jointly with Jacobs University of Bremen. We have also designed a distributed monitoring architecture in the context of advanced measurement infrastructures. These results are presented in section 6.3.5. In addition, we have continued efforts with University of Twente on extending IP flow-based network monitoring with location information. These ones have been centered on additional use cases, applicability of associating IP Flows with metering processes location, and implementation guidelines from both metering process and collector sides.

We have also pursued activities on automated configuration and repair, with a particular focus on safe configuration and service orchestration issues, which are covered in section 6.3.1.

8.4. International Initiatives

8.4.1. Inria International Labs

- LIRIMA (Laboratoire international de recherche en informatique et mathématiques appliquées): MADYNES is associated with the MASECNESS research team of the Yaoundé University in Cameroun. The collaboration is about wireless sensors networks and was the support for funding student mobility (3 months this year). The LIRIMA has also supported the purchase of thirty sensors used in our common work.

8.4.2. Inria International Partners

8.4.2.1. Declared Inria International Partners

- JFLI (CNRS UMI 3527) in Tokyo: Thomas Silverston is currently in this lab (délégation) in Tokyo. The main goal of his research work is to anticipate the evolution of the Internet and to focus on the design of new architectures for the Future Internet. His research program at the JFLI (CNRS, UMI 3527) focus on the use of SDN to allow deploying new network architecture and functionalities in virtualized environment (e.g., ICN) as well as providing a management plane to help network operators monitoring novel network architecture for the Future Internet.

- University of Luxembourg: we have several active cooperations with the university of Luxembourg around network security, Information Centric Networking and Software Defined Networking. Especially, we have one ongoing Ph.D. candidate (Samuel Marchal) and Jérôme François is a Fellow at SnT (Interdisciplinary Center for Security, Reliability and Trust) to empower these collaborations. Besides S. Marchal, we are working particularly with Radu State, Thomas Engel and Salvatore Signorello.

8.4.2.2. Informal International Partners

- University of Twente, The Netherlands, joint work with Professor Aiko Pras on large scale network monitoring and attack detection
- Jacobs University Bremen, joint PhD. with Professor Schoenwaelder on security management in wireless sensor networks
- Federal University of Rio Grande do Sul (UFRGS), joint work with Professor Granville on autonomic management systems
- University of the Federal Armed Forces, Munich Germany, joint work with Professor Gabi Dreo on cloud and mobile cloud security management
- Politecnico di Milano, Italy, joint work with Professor Antonio Capone and Giuliana Carello on energy-aware network management and cloud infrastructures
- Polytecnique de Montrèal, Canada, joint work with Professor Brunilde Sansò on energy-aware network management
- IASI-CNR (National Italian Center of Research), Italy, joint work with Sara Mattia on optimization methods for energy-aware survivable networks
- Zhejiang University (China), joint ANR-NSFC Quasimodo project with professors Youxian Sun, Jiming Chen and Zhi Wang on the adaptive QoS in WSN and multi-target tracking.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

8.5.1.1. Internships

Pedro Paulo Martins Dos Santos

Subject: Flow-based malware signatures

Date: from Jun 2014 to Aug 2014

Institution: Universidade de Brasília, Brazil

8.5.1.2. Scientific visits

Participant: Raouf Boutaba.

Visiting Professor

Network and cloud managements

Date: from Jul to Aug 2014

University of Waterloo, Canada

Participant: Lamia Fourati-Chaari.

Visiting Assistant Professor

Content Centric Networks

Date: from mid-June to end June 2014

Institut d'Informatique et de Multimédia de Sfax (Tunisie)

Participant: Celia Ouanteur.

Visiting PhD student

Markov modeling of Low Latency Deterministic Networks (LLDN) of IEEE802.15.4e

Date: from May to June 2014

University A/Mira of Bejaia, Algeria

Participant: Xiufang Shi.

Visiting PhD student

ANR-NSFC Quasimodo joint project: multi-target location algorithm design

Date: from March to June 2014

Zhejiang University, China

Participant: Shuguo Zhuo.

Visiting PhD student

ANR-NSFC Quasimodo joint project: implementation of iQueue-MAC protocol on RIOT OS

Date: from May to August 2014

Zhejiang University, China

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. General chair, scientific chair, session chair

- Abdelkader Lahmadi: CSSMA Symposium – ICC 2014 (session chair), IEEE/IFIP International Workshop on Management of the Future Internet – MANFI (session chair)
- Bernardetta Addis: 2014 10th International Conference on Modeling, Optimization and SIMulation – Mosim (session chair)
- Jérôme François: IFIP/IEEE International Symposium on Integrated Network Management – IM (session chair)

9.1.1.2. Organizing committee membership

- Rémi Badonnel: IEEE Global Information Infrastructure and Networking Symposium (IEEE GIIS'14), IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM'15)

9.1.2. Scientific events selection

9.1.2.1. Conference program committee chairing

- Rémi Badonnel: IEEE Global Information Infrastructure and Networking Symposium - Special Track on Cloud Infrastructures and Networking (IEEE GIIS'14), IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM'15)
- Thomas Silverston: Crowdsensing 2014

9.1.2.2. Conference program committee membership

- Abdelkader Lahmadi: IEEE/IFIP International Workshop on Management of the Future Internet (MANFI'14), Crowdsensing 2014
- Françoise Simonot-Lion: 10th IEEE International Workshop on Factory Communication Systems (WFCS 2014).
- Isabelle Chrisment: International Conference on Applied Cryptography and Network Security (ACNS'14), IFIP International Conference on Autonomous Infrastructures, Management and Security (IFIP AIMS'14), IFIP International Conference on Communications and Multimedia Security (IFIP CMS'14), International Conference on Advanced Networking, Distributed Systems and Applications (INDS'14), IFIP/IEEE International Symposium on Network Operations and Management (IEEE NOMS'14); National conference on Sécurité des Architectures Réseaux et des Systèmes d?Information (SARSSI 2014- Member of the Steering Committee).
- Jérôme François: 8th IFIP International Conference on Autonomous Infrastructure, Management and Security – AIMS, IEEE/IFIP Network Operations and Management Symposium – NOMS, Cyber Security Analytics and Automation colocated with ACM CCS, European Wireless, Principles, Systems and Applications of IP Telecommunications – IPTComm, Global Information Infrastructure and Networking Symposium – GIIS
- Rémi Badonnel: IFIP/IEEE International Symposium on Network Operations and Management (IEEE NOMS'14), IEEE Global Information Infrastructure and Networking Symposium (IEEE GIIS'14), IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM'15), IFIP International Conference on Autonomous Infrastructures, Management and Security (IFIP AIMS'14), IEEE International Conference on Consumer Communications and Networking (IEEE CCNC'15), Conference on Services and Networks Management (GRES'14), International Workshop on Software Defined Networking and Network Function Virtualisation (IEEE ManSDN/NFV'14), IFIP/IEEE International Workshop on Future Internet Management (IFIP/IEEE MANFI'14), Rencontres Francophones sur l'Algorithmique des Té´lécoms (ALGOTEL'14)
- Ye-Qiong Song: 19th IEEE international conference on Emerging Technologies & Factory Automation (ETFA'2014) - Industrial communication systems track ; 12th International Conference On Smart homes and health Telematics (ICOST 2014); 13th International Workshop on Real-Time Networks (RTN 2014); 10th IEEE International Workshop on Factory Communication Systems (WFCS 2014); 7th IFIP Wireless and Mobile Networking Conference (WMNC 2014); 12th International Conference on Embedded Computing (EmbeddedCom 2014); 2nd International Workshop on compressive Sensing in Cyber-Physical Systems, Co-located with the 11th IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS 2014).

9.1.2.3. Reviewing activities

- Abdelkader Lahmadi: IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM'15), Special Track on the Management of the Internet of Things (IEEE NOMS'14).
- Bernardetta Addis: 2014 10th International Conference on Modeling, Optimization and SIMulation (Mosim), 2015 IEEE 12th Consumer Communications and Networking Conference (CCNC)
- Françoise Simonot-Lion: 10th IEEE International Workshop on Factory Communication Systems (WFCS 2014).
- Isabelle Chrisment: International Conference on Applied Cryptography and Network Security (ACNS'14), IFIP International Conference on Autonomous Infrastructures, Management and Security (IFIP AIMS'14), IFIP International Conference on Communications and Multimedia Security (IFIP CMS'14), International Conference on Advanced Networking, Distributed Systems and Applications (INDS'14), IFIP/IEEE International Symposium on Network Operations and Management (IEEE NOMS'14).
- Emmanuel Nataf: SENSORSNET 2015

- Rémi Badonnel: IFIP/IEEE International Symposium on Network Operations and Management (IEEE NOMS'14), IEEE Global Information Infrastructure and Networking Symposium (IEEE GIIS'14), IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM'15), IFIP International Conference on Autonomous Infrastructures, Management and Security (IFIP AIMS'14), IEEE International Conference on Consumer Communications and Networking (IEEE CCNC'15), Conference on Services and Networks Management (GRES'14), International Workshop on Software Defined Networking and Network Function Virtualisation (IEEE ManSDN/NFV'14), IFIP/IEEE International Workshop on Future Internet Management (IFIP/IEEE MANFI'14), Rencontres Francophones sur l'Algorithmique des Télécoms (ALGOTEL'14)
- Thibault Cholez: Applied Cryptography and Network Security 2014, IFIP/IEEE International Symposium on Network Operations and Management (IEEE NOMS'14), IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM'15), IEEE International Conference on Communications (ICC'15)
- Ye-Qiong Song: 19th IEEE international conference on Emerging Technologies & Factory Automation (ETFA'2014) - Industrial communication systems track ; 12th International Conference On Smart homes and health Telematics (ICOST 2014); 13th International Workshop on Real-Time Networks (RTN 2014); 10th IEEE International Workshop on Factory Communication Systems (WFCS 2014); 7th IFIP Wireless and Mobile Networking Conference (WMNC 2014); 12th International Conference on Embedded Computing (EmbeddedCom 2014); 2nd International Workshop on compressive Sensing in Cyber-Physical Systems, Co-located with the 11th IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS 2014).

9.1.3. Journal

9.1.3.1. Editorial board membership

- Françoise Simonot-Lion: IEEE Transactions on Industrial Informatics (associated editor).
- Ye-Qiong Song: Elsevier Computers and Electrical Engineering journal (associate editor); Journal of Multimedia Information System (associate editor).

9.1.3.2. Reviewing activities

- Abdelkader Lahmadi: Springer's Journal of Network and Systems Management (JNSM), IEEE Communications Magazine, IEEE Transactions on Network and Service Management (TNSM), International Journal of Network Management (IJNM).
- Bernardetta Addis: Computer Communications, Computers and Operations Research, Computational Optimization and Applications, Discrete and Applied Mathematics, European Journal of Operations Research, Journal of Combinatorial Optimization, Journal of Global Optimization, Mathematical Methods of Operations Research, IEEE/ACM Transactions on Networking
- Françoise Simonot-Lion: Journal Mathematical Problem in Engineering, IEEE Transactions on Industrial Informatics.
- Isabelle Chrisment: IEEE Communications Magazine, Security and Communication Networks, Computer Networks, Privacy in a Digital, Networked World -Technologies, Implications and Solutions (book) , ARIMA Journal (Revue Africaine de la Recherche en Informatique et Mathématiques Appliquées)
- Jérôme François: IEEE Transactions on Network and Service Management, Elsevier Computer Networks, International Journal of Network Management – IJNM
- Rémi Badonnel: IEEE Transactions on Network and Service Management (IEEE TNSM), Springer's Journal of the Network and Systems Management (JNSM)
- Thibault Cholez: IEEE Transactions on Network and Service Management, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Computers, Elsevier Computer Networks, Journal of Communications and Networks

- Ye-Qiong Song: Elsevier Computers and Electrical Engineering journal (associate editor); Journal of Multimedia Information System (associate editor); IEEE Transactions on Industrial Informatics; Journal of distributed sensor networks; IEEE Transactions on Cloud Computing; ACM Transactions on Architecture and Code Optimization.

9.1.4. Other animation activities

Isabelle Chrisment is a member of AFNIC scientific board since January 2013

Isabelle Chrisment is the Co-Chair together with Ahmed Serhrouchni from Telecom ParisTech of the IFIP Task Force 6.5 on Secure Networking. This Task Force provides a framework for the organization of activities within the scope of secure networking. It facilitates international cooperation activities and exchanges in this area.

Olivier Festor is Chair of the IFIP Working-Group 6.6 on Network and systems management. This working group is actively involved the animation of most major conferences in this research area and organizes frequent meetings and workshops on the domain.

Olivier Festor is the Co-chair together with Lisandro Zambenedetti Grandvile from the Federal University of Rio Grande do Sul (UFRGS) of the Internet Research Task Force (IRTF) Network Management Research Group since march 2011.

Françoise Simonot-Lion is Scientific Delegate with HCERES.

Françoise Simonot-Lion was member of the review panel of the research evaluation at Mälardalen University (May 2014).

Françoise Simonot-Lion was chair of the review panel of the research evaluation of Department DTIM at ONERA (December 2014).

Ye-Qiong Song is the member of the jury of the Gilles Kahn best PhD thesis award.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

There is a high demand on networking courses in the various universities in which LORIA is part of. This puts high pressure on MADYNES members which are all in charge of numerous courses in this domain. Especially the team professors and associate professors ensure more than the required amount of teaching obligation in their respective institutions: IUT, bachelor, master, TELECOM Nancy, ENSEM and École des Mines de Nancy engineering schools.

Laurent Andrey was the Head of Department of the Charlemagne IUT specialization on multimedia networking until the end of the academic year 2014.

Olivier Festor is the Director of the TELECOM Nancy Engineering School. Remi Badonnel is heading the Telecommunications and Networks specialization of the 2nd and 3rd years at the TELECOM Nancy engineering school, and is also in charge of the 2nd year design and development projects at the same school. They teach the networking related courses in this cursus.

Isabelle Chrisment was co-directing the school and in charge of the students recruitment process until September 2014.

Laurent Ciarletta is heading the specialization Safe Systems Architecture of the Computer Science and IT department of the Ecole des Mines de Nancy ("Grande Ecole", Engineering School, Master degree level). He is most notably in charge of Advanced Networking, Middleware, Component-based software development, Pervasive Computing, Networking and Systems courses at the Ecole des Mines de Nancy. Notably, within the ARTEM alliance (ICN - Business School, Mines Nancy, Ecole d'Art / School of Art), he is a member of the Research Committee, more specifically with the "Smart Working Spaces" research theme, and he is co-responsible for the "Businesses: the digital challenge *CORP 3.0, Entreprises: le défi numérique* and the *Imagineries and the Workspaces*, 2 classes within the ARTEM alliance (over 90 hours).

Thomas Silverston was in charge of the SSSR Master degree at IGA (Morroco).

Team members are teaching the following courses:

Abdelkader Lahmadi

- 280 hours
- Level: Engineering degree (L1, M1, M2)
- Algorithms and Java programming, C language programming, Real Time systems, Databases, Distributed algorithms, constrained systems programming
- ENSEM - Engineering school

Bernardetta Addis

- 158 hours
- Level: M2
- Operations Research, Discrete Optimization
- Ecoles de Mines de Nancy

Isabelle Chrisment

- 220 hours
- Engineering/Master Degree in Computer Science
- C and Shell Programing, Computer Networking, Operating Systems, Network Security.
- TELECOM Nancy Engineering School of Computer Science

Jérôme François

- 28 hours
- Master 2
- Network security, Hadoop
- Univ. Lorraine, Telecom Nancy

Emmanuel Nataf

- 192 hours
- L1 L2 M2
- Network, operating system, network monitoring
- IUT Nancy-Charlemagne, Telecom Nancy, Université de Lorraine

Olivier Festor

- 192 hours
- Engineering/Master Degreee in Computer Science
- Network, Programming, Algorithmics, Complexity
- TELECOM Nancy Engineering School of Computer Science

Rémi Badonnel

- 242 hours
- Engineering/Master Degree in Computer Science
- Networks, Systems and Services, Network Management, Software Design and Programming, Cloud Computing
- TELECOM Nancy Engineering School of Computer Science

Thibault Cholez

- 258 hours
- Level: Engineering/Master Degree in Computer Science (L2, M1, M2)

- Main topics: Computer Networks, Databases, Object-Oriented Programming, C and Shell Programming, Techniques and Tools for Programming, Network Services, Constraint development on small Connected Objects, Mobile applications and Internet of Things.
- Main location: TELECOM Nancy Engineering School in Computer Science

Thomas Silverston

- 300 hours
- Level: Master Degree in Computer Science
- Networking, Network Security and VoIP
- Main location: University of Lorraine

Ye-Qiong

- 242 hours
- Level: Engineering degree (L1, M1, M2)
- Algorithms and Java programming, networking, Databases, sensor networks.
- ENSEM - Engineering school

E-learning

MOOC, Introduction to Nagios-based Monitoring (45 minutes, English), Flamingo Network of Excellence, 8900 views in less than 1 year.

9.2.2. Supervision

PhD: Martin Barrere, Vulnerability Management in Autonomic Networks and Systems, University of Lorraine, since Jun 2014, supervised by Olivier Festor, Rémi Badonnel

PhD in progress: Elian Aubry, Using Software Defined Network to manage Content Centric Networks, since October 2013, supervised by Isabelle Chrisment, Thomas Silverston.

PhD in progress: César Bernardini, Réseau orienté-contenu basé sur les communautés d'utilisateurs, since Nov 2011, supervised by Olivier Festor et Thomas Silverston

PhD in progress: Francois Despaux, QoS in wireless sensor and actuator networks, since November 2011, supervised by Ye-Qiong Song, Abdelkader Lahmadi

PhD in progress: Gaëtan Hurel, Mobile Cloud Security, since Jan 2014, supervised by Olivier Festor, Rémi Badonnel, Abdelkahder Lahmadi

PhD in progress: Patrick-Olivier Kamgue, Routing management in WSNs, since Jun 2012, supervised by Emmanuel Nataf and Olivier Festor in France, Thomas Djotio in Cameroun

PhD in progress: Samuel Marchal, honeypot and malware analysis, since October 2013, supervised by Olivier Festor in France, Thomas Engel in Luxembourg

PhD in progress: Anthéa Mayzaud, Monitoring ans Security for the Internet of Things, since May 2013, supervised by Isabelle Chrisment, Rémi Badonnel

PhD in progress: Kevin Roussel : Dynamic management of QoS and energy in heterogenous sensor and actuator networks for e-health applications, since Dec 2012, supervised by Ye-Qiong Song

PhD in progress : Mohamed Said Seddiki, Allocation des ressource dans la virtualisation des réseaux, since Mar 2013, supervised by Ye-Qiong Song, and by Mounir Frikha in Tunisia

PhD in progress: Evangelia Tsiontsiou , Multiconstrained QoS routing for wireless sensors networks with applications to smart space for ambient assisted living, since October 2013, supervised by Ye-Qiong Song, Bernardetta Addis

PhD in progress: Shbair Wazen, Contributions for the Management of HTTPS traffic, since December 2013, supervised by Isabelle Chrisment and Thibault Cholez

9.2.3. Juries

Team members participated to the following Ph.D. defense committees:

- Tristan Groléat, Ph.D. in Computer Science from Université Européenne de Bretagne, Télécom Bretagne Title: High Performance traffic monitoring for network security and management, March 2014 – (Isabelle Chrisment)
- Truong Khoa Phan, Ph.D. in Computer Science from Université de Nice - Sophia Antipolis. Title: Design and Management of Networks with Low Power Consumption, September 2014 – (Bernardetta Addis)
- Houari Mahfoud, Ph.D. in computer science from Université de Lorraine. Title: Efficient Access Control to XML Data: Querying and Updating Problems, Feb. 2014 – (Ye-Qiong Song)
- Nadine Abdallah, Ph.D. in control and applied computer science from Université de Nantes. Title: Multiprocessor real-time partitioning with Quality of Service requirements and energy constraints, Feb. 2014 – (Ye-Qiong Song)
- Ridha Soua, Ph.D. in comupter science from Université Pierre et Marie Curie Paris 6. Title: Wireless Sensor Networks in Industrial Environment: Energy Efficiency, Delay and Scalability, Feb. 2014 – (Ye-Qiong Song)
- William Mangoua Sofack, Ph.D. in computer science from Université de Toulouse. Title: Amélioration des délais de traversés pire cas des réseaux embarqués à l'aide du calcul réseau, June 2014 – (Ye-Qiong Song)
- Philippe Thierry, Ph.D. in computer science from Université Paris-Est. Title: Systè`mes véhiculaires à` domaines de sécurité et de criticité multiples : une passerelle systronique, July 2014 – (Ye-Qiong Song)
- Hamdi Ayed, Ph.D. in networking, telecommunications, systems and architectures from Université de Toulouse. Title: Analysis and optimization of multi-cluster avionics networks, November 2014 – (Ye-Qiong Song)
- Yan Han, Ph.D. in computer science from Université de Rennes 1. Title: Smart devices collaboration for energy saving in home networks, December 2014 – (Ye-Qiong Song)

Team members acted as reviewer for the following Ph.D. thesis:

- Inad Nawajah, Ph.D. in Mathematical Models and Methods in Engineering from Politecnico di Milano. Title: Bayesian Analysis of home care longitudinal counts data, 2014 – (Bernardetta Addis)
- Wei You, Ph.D. in Computer Science from Université Européenne de Bretagne, Télécom Bretagne Title: A Content-Centric Networking Node for a Realistic Efficient Implementation and Deployment, January 2014 – (Isabelle Chrisment)
- Antoine Lavignotte, Ph.D. in Computer Science from Université de Saint-Etiienne Title: Prise en compte de la qualité de l'expérrance utilisateur au sein des protocoles de streaming adaptatifs, Mai 2014 – (Isabelle Chrisment)
- Silvia Gil Casals, Ph.D. in Computer Science from Université de Toulouse, Title: Risk Assessment and Intrusion Detection for Airborne Networks, July 2014 – (Isabelle Chrisment)
- Rim Moalla, Ph.D. in Computer Science from Télécom ParisTech and Université Pierre et Marie Curie. Title: Secure Future Cooperative ITS Applications, (September 2014) – (Isabelle Chrisment)
- Ludie Akue, Ph.D. in COmputer Science from Université de Toulouse, Title: Un cadriciel pour la vérification en ligne, générique, flexible et évolutive de configurations de systèmes communicants complexes, (February 2014) – (Olivier Festor)
- Raphael Barbosa, Ph.D. in Computer Science from University of Twente, Title: Anomaly Detection in SCADA systems, (Febrary 2014) – (Olivier Festor)
- Rebecca Steinert, Ph.D. in Computer Science from KTH, Title: Probabilistic Fault Management in Networked Systems, (June 2014) – (Olivier Festor)
- Anthony Dessiatnikoff, Ph.D. in Computer Science from Université de Toulouse, Title: Analyse de Vulnérabilités de systèmes avioniques embarqués: classification et expérimentation, (June 2014) – (Olivier Festor)

- Ghida Ibrahim, Ph.D. in Computer Science and Networking from TELECOM ParisTech, Title: Evolution of the Control Plane for Future Content Distribution Services, (june 2014) – (Olivier Festor)
- Ahmed Amokrane, PhD in Computer Science from Pierre et marie Curie University Title: Green et Effcacité en Energie dans les Réseaux d'Accès et Infrastructures Cloud, ((December 2014) – (Olivier Festor)
- Ridha Soua, Ph.D. in comupter science from UNIVERSITY PARIS 6 PIERRE ET MARIE CURIE. Title: Wireless Sensor Networks in Industrial Environment: Energy Efficiency, Delay and Scalability, Feb. 2014 – (Ye-Qiong Song)
- William Mangoua Sofack, Ph.D. in computer science from Université de Toulouse. Title: Amélioration des délais de traversés pire cas des réseaux embarqués à l'aide du calcul réseau, June 2014 – (Ye-Qiong Song)
- Philippe Thierry, Ph.D. in computer science from Université Paris-Est. Title: Systèmes véhiculaires à domaines de sécurité et de criticité multiples : une passerelle systronique, July 2014 – (Ye-Qiong Song)
- Hamdi Ayed, Ph.D. in networking, telecommunications, systems and architectures from Université de Toulouse. Title: Analysis and optimization of multi-cluster avionics networks, November 2014 – (Ye-Qiong Song)
- Yan Han, Ph.D. in computer science from Université de Rennes 1. Title: Smart devices collaboration for energy saving in home networks, December 2014 – (Ye-Qiong Song)

Team members participated to the following Habilitation Degree defense committees:

- Stefano Secci, , Habilitation Degree in Computer Science from Pierre et Marie Curie - Paris 6 University. Title: Modeling and Evaluating Novel Networked Communications Systems, (September 2014) – (Olivier Festor)
- (Liliana Cucu-Grosjean), Habilitation Degree in (Computer Science) from (Université Paris 6). Title: (Contributions to real-time systems), (May 2014) — (Françoise Simonot-Lion)

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] M. BARRERE. *Vulnerability Management for Safe Configurations in Autonomic Networks and Systems*, Université de Lorraine, June 2014, https://hal.inria.fr/tel-01095206

Articles in International Peer-Reviewed Journals

[2] B. ADDIS, D. ARDAGNA, G. CARELLO, A. CAPONE. *Energy-aware joint management of networks and Cloud infrastructures*, in "Computer Networks and ISDN Systems", September 2014, pp. 75–95, http://www.sciencedirect.com/science/article/pii/S1389128614001649, https://hal.archives-ouvertes.fr/hal-01088593

[3] B. ADDIS, G. CARELLO, A. CAPONE, L. G. GIANOLI, B. SANSÒ. *Energy management through optimized routing and device powering for greener communication networks*, in "IEEE/ACM Transactions on Networking", February 2014, vol. 22, n^{o} 1, pp. 313-325, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6490068, https://hal.archives-ouvertes.fr/hal-01088564

[4] B. ADDIS, G. CARELLO, A. CAPONE, L. G. GIANOLI, B. SANSÒ. *On the energy cost of robustness and resiliency in IP networks*, in "Computer Networks and ISDN Systems", December 2014, pp. 239-259, http://www.sciencedirect.com/science/article/pii/S1389128614003594, https://hal.archives-ouvertes.fr/hal-01088614

[5] R. FOURNIER, T. CHOLEZ, M. LATAPY, I. CHRISMENT, C. MAGNIEN, O. FESTOR, I. DANILOFF. *Comparing Pedophile Activity in Different P2P Systems*, in "Social Sciences", July 2014, vol. 3, n° 3, pp. 314-325 [*DOI :* 10.3390/SOCSCI3030314], https://hal.inria.fr/hal-01052773

[6] D. IZZO, L. F. SIMÕES, C. H. YAM, F. BISCANI, D. DI LORENZO, B. ADDIS, A. CASSIOLI. *GTOC5: Results from the European Space Agency and University of Florence*, in "ACTA Futura", 2014, pp. 45-55, http://www.esa.int/gsp/ACT/doc/ACTAFUTURA/AF08/papers/AF08.2014.45.pdf, https://hal.archives-ouvertes.fr/hal-01088586

[7] J. LI, Y.-Q. SONG, X. LIU. *Introduction to special issue on Embedded Computing and Systems*, in "Computers and Electrical Engineering", July 2014, vol. 40, n° 5, pp. 1564-1566, https://hal.archives-ouvertes.fr/hal-01093662

[8] S. MARCHAL, J. FRANÇOIS, R. STATE, T. ENGEL. *PhishStorm: Detecting Phishing with Streaming Analytics*, in "IEEE Transactions on Network and Service Management", December 2014, 14 p. [*DOI :* 10.1109/TNSM.2014.2377295], https://hal.inria.fr/hal-01092771

International Conferences with Proceedings

[9] Y. ABID, B. SAADALLAH, A. LAHMADI, O. FESTOR. *Named data aggregation in wireless sensor networks*, in "IEEE Network Operations and Management Symposium (NOMS)", Cracovie, Poland, May 2014, pp. 1 - 8 [*DOI :* 10.1109/NOMS.2014.6838364], https://hal.inria.fr/hal-01092025

[10] M. BARRERE, R. BADONNEL, O. FESTOR. *A SAT-based Autonomous Strategy for Security Vulnerability Management*, in "IEEE/IFIP International Symposium on Network Operations and Management (IEEE/IFIP NOMS'14)", Cracovie, Poland, May 2014, https://hal.inria.fr/hal-01093121

[11] C. BERNARDINI, T. SILVERSTON, O. FESTOR. *Socially-Aware Caching Strategy for Content Centric Networking*, in "IFIP Networking 2014", Trondheim, Norway, June 2014, https://hal.inria.fr/hal-01111616

[12] L. CIARLETTA, L. GILPIN, Y. PRESSE, V. CHEVRIER, V. GALTIER. *Co-simulation Solution using AA4MM-FMI applied to Smart Space Heating Models*, in "7th International ICST Conference on Simulation Tools and Techniques", Lisbon, Portugal, March 2014, https://hal.inria.fr/hal-00966461

[13] L. CIARLETTA, A. GUENARD, Y. PRESSE, V. GALTIER, Y.-Q. SONG, J.-C. PONSART, S. ABERKANE, D. THEILLIOL. *Simulation and platform tools to develop safe flock of UAVs: a CPS application-driven research*, in "ICUAS - International Conference on Unmanned Aircraft Systems", Orlando, Floride, United States, May 2014, pp. 95-102 [*DOI :* 10.1109/ICUAS.2014.6842244], https://hal.archives-ouvertes.fr/hal-01059310

[14] F. DESPAUX, Y.-Q. SONG, A. LAHMADI. *Modelling and Performance Analysis of Wireless Sensor Networks Using Process Mining Techniques: ContikiMAC Use Case*, in "DCOSS 2014", Marina del Rey, United States, May 2014, pp. 1 - 8 [*DOI :* 10.1109/DCOSS.2014.20], https://hal.inria.fr/hal-01093736

[15] F. DESPAUX, Y.-Q. SONG, A. LAHMADI. *Towards performance analysis of wireless sensor networks using Process Mining Techniques*, in "ISCC", Madère, Portugal, June 2014, pp. 1 - 7 [*DOI :* 10.1109/ISCC.2014.6912522], https://hal.inria.fr/hal-01093729

[16] E. FINICKEL, A. LAHMADI, F. BECK, O. FESTOR. *Empirical analysis of Android logs using self-organizing maps*, in "ICC 2014 : IEEE International Conference on Communications", Sydney, Australia, IEEE, June 2014, pp. 1802 - 1807 [*DOI :* 10.1109/ICC.2014.6883584], https://hal.inria.fr/hal-01092011

[17] J. FRANÇOIS, L. DOLBERG, O. FESTOR, T. ENGEL. *Network Security through Software Defined Networking: a Survey*, in "IIT Real-Time Communications (RTC) Conference - Principles, Systems and Applications of IP Telecommunications (IPTComm)", Chicago, United States, ACM, September 2014, https://hal.inria.fr/hal-01087248

[18] J. FRANÇOIS, O. FESTOR. *Anomaly Traceback using Software Defined Networking*, in "International Workshop on Information Forensics and Security", Atlanta, United States, IEEE, December 2014, https://hal.inria.fr/hal-01092789

[19] G. HUREL, R. BADONNEL, A. LAHMADI, O. FESTOR. *Outsourcing Mobile Security in the Cloud*, in "8th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security - AIMS", Brno, Czech Republic, Monitoring and Securing Virtualized Networks and Services, Springer, June 2014, vol. 8508, pp. 69 - 73 [*DOI :* 10.1007/978-3-662-43862-6_9], https://hal.inria.fr/hal-01092239

[20] S. MARCHAL, J. FRANÇOIS, R. STATE, T. ENGEL. *PhishScore: Hacking Phishers' Minds*, in "International Conference on Network and Service Management", Rio de Janeiro, Brazil, IEEE, November 2014, https://hal.inria.fr/hal-01094238

[21] *Best Paper*
A. MAYZAUD, A. SEHGAL, R. BADONNEL, I. CHRISMENT, J. SCHÖNWÄLDER. *A Study of RPL DODAG Version Attacks*, in "8th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2014", Brno, Czech Republic, June 2014, pp. 92 - 104, Best Paper Award [*DOI :* 10.1007/978-3-662-43862-6_12], https://hal.inria.fr/hal-01090993.

[22] T. NAVARRETE, L. CIARLETTA, V. CHEVRIER. *A control architecture of complex systems based on multi-agent models*, in "Conference on Practical Applications of Agents and Multi-Agent Systems", Salamenque, Spain, June 2014, https://hal.inria.fr/hal-00966467

[23] T. NAVARRETE, L. CIARLETTA, V. CHEVRIER. *Multi-agent Simulation based control of complex systems*, in "International Conference on Autonomous Agents and Multiagent Systems", PARIS, France, May 2014, https://hal.inria.fr/hal-00966436

[24] M. S. SEDDIKI, M. SHAHBAZ, S. DONOVAN, S. GROVER, M. PARK, N. FEAMSTER, Y.-Q. SONG. *FlowQoS: QoS for the Rest of Us*, in "ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN'2014)", Chicago, United States, August 2014 [*DOI :* 10.1145/2620728.2620766], https://hal.archives-ouvertes.fr/hal-01071445

[25] A. SEHGAL, A. MAYZAUD, R. BADONNEL, I. CHRISMENT, J. SCHÖNWÄLDER. *Addressing DODAG inconsistency attacks in RPL networks*, in "Global Information Infrastructure and Networking Symposium

(GIIS)", Montreal, QC, Canada, September 2014, pp. 1 - 8 [*DOI :* 10.1109/GIIS.2014.6934253], https://hal.inria.fr/hal-01090986

[26] J. P. TIMPANARO, I. CHRISMENT, O. FESTOR. *Group-Based Characterisation for the I2P Anonymous File-Sharing Environment*, in "New Technologies, Mobility and Security - NTMS", Dubai, United Arab Emirates, March 2014, https://hal.inria.fr/hal-00986228

[27] C. ZHAO, W. ZHANG, X. YANG, Y. YANG, Y.-Q. SONG. *A novel compressive sensing based Data Aggregation Scheme for Wireless Sensor Networks*, in "IEEE international conference on Communications (ICC)", Sidney, Australia, IEEE, June 2014, https://hal.archives-ouvertes.fr/hal-01093644

National Conferences with Proceedings

[28] A. MAYZAUD, A. SEHGAL, R. BADONNEL, I. CHRISMENT. *Gestion de risques appliquée aux réseaux RPL*, in "9ème Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information", Saint-Germain-Au-Mont-d'Or, France, May 2014, https://hal.inria.fr/hal-01091008

Conferences without Proceedings

[29] B. ADDIS, G. CARELLO, S. MATTIA. *Energy-aware survivable network management with shared protection*, in "ROADEF - 15ème congrès annuel de la Société française de recherche opérationnelle et d'aide à la décision", Bordeaux, France, Société française de recherche opérationnelle et d'aide à la décision, February 2014, https://hal.archives-ouvertes.fr/hal-00946371

[30] C. BERNARDINI, T. SILVERSTON, O. FESTOR. *A Pin is Worth a Thousand Words: Characterization of Publications in Pinterest*, in "5th International Workshop on TRaffic Analysis and Characterization", Nicosia, Cyprus, IEEE, August 2014, https://hal.inria.fr/hal-01111630

[31] A. GROSSO, B. ADDIS, G. CARELLO, E. TÀNFANI. *A rolling horizon framework for the OR planning under uncertain surgery duration: deterministic versus robust approach*, in "ROADEF - 15ème congrès annuel de la Société française de recherche opérationnelle et d'aide à la décision", Bordeaux, France, Société française de recherche opérationnelle et d'aide à la décision, February 2014, https://hal.archives-ouvertes.fr/hal-00946363

[32] G. HUREL, R. BADONNEL, A. LAHMADI, O. FESTOR. *Towards Cloud-Based Compositions of Security Functions For Mobile Devices*, in "IFIP/IEEE International Symposium on Integrated Network Management (IM'15)", Ottawa, Canada, May 2015, 6 p. , https://hal.inria.fr/hal-01093041

Scientific Books (or Scientific Book chapters)

[33] T. CHOLEZ, G. DOYEN, I. CHRISMENT, O. FESTOR, R. KHATOUN. *Faiblesses de l'identification dans les espaces numériques ouverts de partage de contenus : le cas des réseaux pair-à-pair*, in "Enseignement, préservation et diffusion des identités numériques", J.-P. PINTE (editor), Traité des sciences et techniques de l'information, Hermès - Lavoisier, May 2014, https://hal.inria.fr/hal-01052851

[34] D. SIMON, Y.-Q. SONG, O. SENAME. *Conception conjointe commande-ordonnancement*, in "Ordonnancement dans les systèmes temps réel", M. CHETTO (editor), ISTE Editions, June 2014, pp. 293-324, http://hal-lirmm.ccsd.cnrs.fr/lirmm-01017944

[35] D. SIMON, Y.-Q. SONG, O. SENAME. *Control and Scheduling Joint Design*, in "Real-time Systems Scheduling", M. CHETTO (editor), ISTE Editions, September 2014, vol. 2 "Focuses", pp. 53-96, http://hal-lirmm.ccsd.cnrs.fr/lirmm-01067487

[36] Y.-Q. SONG. *L'ordonnancement dans les réseaux*, in "Ordonnancement dans les systèmes temps réel", ISTE Editions, July 2014, https://hal.archives-ouvertes.fr/hal-01093665

[37] Y.-Q. SONG. *Scheduling in Networks*, in "Real-time Systems Scheduling 2 : Focuses", Real-time Systems Scheduling 2 : Focuses, ISTE, August 2014, vol. 2, https://hal.archives-ouvertes.fr/hal-01093667

Other Publications

[38] Y. ABID. *Modélisation et analyse de l'impact des cyber-attaques sur les systèmes SCADA*, Université de Lorraine, September 2014, https://hal.inria.fr/hal-01093741

[39] B. ADDIS, G. CARELLO, A. GROSSO, E. TÀNFANI. *A rolling horizon framework for the operating rooms planning under uncertain surgery duration*, 2014, https://hal.archives-ouvertes.fr/hal-00936085

[40] B. ADDIS, G. CARELLO, E. TÀNFANI. *A robust optimization approach for the Advanced Scheduling Problem with uncertain surgery duration in Operating Room Planning - an extended analysis*, 2014, https://hal.archives-ouvertes.fr/hal-00936019

[41] F. BAKLOUTI. *Analysis and visualisation of network data flows of Android applications*, ENSI Tunisie, October 2014, https://hal.inria.fr/hal-01093731

[42] R. CHEVALIER. *Etude de la cartographie des systèmes SCADA à l'échelle d'Internet*, ENS Cachan antenne de Bretagne, Université de Rennes 1, September 2014, https://hal.inria.fr/hal-01095049

[43] A. DEROCHE. *Mise en place d'un service de géolocalisation au sein d'une plateforme d'exploitation d'un réseau de capteurs sans fil*, TELECOM Nancy, September 2014, 31 p. , https://hal.inria.fr/hal-01097784

[44] A. DEROCHE, T. DUHAL. *Mise en œuvre d'un réseau expérimental de capteurs sans fil et application domotique*, Telecom Nancy, May 2014, https://hal.inria.fr/hal-01059027

[45] T. DUHAL. *Mise en œuvre d'un collecte distribuée au moyen du développement d'une plate-forme de gestion pour des réseaux de capteurs sans fil*, Telecom Nancy, September 2014, https://hal.inria.fr/hal-01059038

[46] A. GARNIER, E. NATAF. *Développement d'une plate-forme de supervision d'un réseau de capteurs*, IUT Informatique, Nancy, June 2014, https://hal.inria.fr/hal-01059019

[47] A. GOICHOT. *Étude du filtrage de flux HTTPS*, TELECOM Nancy, September 2014, 38 p. , https://hal.inria.fr/hal-01097781

[48] P. O. KAMGUEU, E. NATAF, T. DJOTIO, O. FESTOR. *Fuzzy-based routing metrics combination for RPL*, January 2014, 8 p. , Doctoral Consortium Sensornets 2014, https://hal.inria.fr/hal-01093965

[49] G. ROBIN. *Détection d'anomalies dans les systèmes SCADA*, ENSEM, February 2014, https://hal.inria.fr/hal-01095048

References in notes

[50] O. FESTOR, A. LAHMADI, R. HOFSTEDE, A. PRAS. *Information Elements for IPFIX Metering Process Location*, July 2013, Internet Draft - IETF, https://hal.inria.fr/hal-00879567

[51] J. SIEBERT. *Approche multi-agent pour la multi-modélisation et le couplage de simulations. Application à l'étude des influences entre le fonctionnement des réseaux ambiants et le comportement de leurs utilisateurs*, Université Henri Poincaré - Nancy I, September 2011, http://tel.archives-ouvertes.fr/tel-00642034