IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2013

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 Scientist

Vassili Rivron [Inria, Researcher on leave from Université de Caen, from Sep 2013]

Faculty Members

Olivier Festor [Team leader, Université de Lorraine, Professor, HdR]
Bernardetta Addis [Université de Lorraine, Associate Professor, from Sep 2013]
Laurent Andrey [Université de Lorraine, Associate Professor]
Rémi Badonnel [Université de Lorraine, Associate Professor]
Thibault Cholez [Université de Lorraine, Associate Professor, from Sep 2013]
Isabelle Chrisment [Université de Lorraine, Professor, HdR]
Laurent Ciarletta [Université de Lorraine, Associate Professor]
Abdelkader Lahmadi [Université de Lorraine, Associate Professor]
Emmanuel Nataf [Université de Lorraine, Associate Professor]
Thomas Silverston [Université de Lorraine, Associate Professor]
Françoise Simonot-Lion [Université de Lorraine, Professor Emeritus]
Ye-Qiong Song [Université de Lorraine, Professor, HdR]

Engineers

Alexandre Boeglin [Inria, FP7 EIT ICT LABS GA project, until Dec 2013]
Moutie Chehaider [Inria, ADT PAL-PERCEE, until Apr 2013]
Eric Finickel [Inria, Ingénieur Jeune Diplomé, from Sep 2013]
Mandar Harshe [Inria, ADT PAL-PERCEE, from Jun 2013]
Gaëtan Hurel [Inria, FP7 UNIVERSELF project, until Dec 2013]
Mohammad Irfan Khan [Inria, ADT Metrocope, since Nov 2013]
Yannick Presse [Inria, Inria-EDF Strategic action, until Dec 2013]
Bilel Saadallah [Inria, FP7 UNIVERSELF project, until Dec 2013]

PhD Students

Elian Aubry [Univ. Lorraine, granted by Ministry or Research, since Oct 2013]
Martin Barrere [Inria, granted by FP7 UNIVERSELF project, since Mar 2011]
César Bernardini [Inria, granted by FP7 UNIVERSELF project and Conseil Régional de Lorraine, since Nov 2011]
Francois 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]
Wazen Shbair [Univ. Lorraine, granted by Erasmus Mundus EPIC, since Dec. 2013]
Juan Pablo Timpanaro [Inria, Université de Lorraine, granted by ANR MAPE project, defended the 6th November 2013]
Evangelia Tsiontsiou [Univ. Lorraine, granted by SATELOR project from AME Lorraine, since Oct 2013]

Administrative Assistants

Delphine Hubert [Univ. Lorraine, from Jan 2013]
Céline Simon [Inria]

Others

Younes Abid [Inria, Intern Master student from ENSI - Tunis, from Mar 2013 until Sep 2013]
Juan Caubet [Visiting PhD Student from Technical University of Catalonia (UPC) from Aug 2013 until Nov 2013]
Narjess Derouiche [Intern Master student from SUP'COM Tunis, from Mar 2013 until Sep 2013]
Benjamin Fuhrmann [Inria, Intern Master student from TELECOM NANCY, from Jun 2013 until Aug 2013]
Leilani Gilpin [Inria, Intern Master student from Stanford University, from Jun 2013 until Sep 2013]
Florian Greff [Inria, Intern Master student from TELECOM NANCY, from Jun 2013 until Aug 2013]
Nicolas Meyer [Univ. Lorraine, Intern Master student from Mines Nancy, from Jul 2013 until Sep 2013]
Fadwa Rebhi [Inria, Intern from ENSI - Tunis, from Mar 2013 until Sep 2013]
Nicolas Schnepf [Inria, Intern License student from IUT Nancy-Charlemagne, from Apr 2013 until Jun 2013]
Ayoub Soury [Inria, Intern Master student, from Feb 2013 until Jun 2013]
Julien Vaubourg [Inria, Intern Master student from TELECOM NANCY, from Mar 2013 until Sep 2013]
Achraf Weslati [Inria, Intern Master student from ENSI - Tunis, from Mar 2013 until Sep 2013]
Ibrahim Yanik [Univ. Lorraine, Intern Master student from ENSEM, from Apr 2013 until Sep 2013]

2. Overall Objectives

2.1. Introduction

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.

2.2. Highlights of the Year

The following points of 2013 deserves to be highlighted:

- Two new permanent members joined the MADYNES team: Bernardetta Addis and Thibault Cholez. They are associate professor at the University of Lorraine with teaching activities at Mines Nancy and TELECOM Nancy, respectively.
- An outstanding publication was achieved in the journal "IEEE Communications Surveys and Tutorials" which has an impact factor of 4.8.
- In relation with research (Aetournos project, R2D2 ADT), the Alérion project has been one of the "15ème concours national de création d'entreprises innovantes" (national innovative startup program) prize-winner in 2013 in the "emerging" category. The Alérion project is offering an e-falconry solution based on interconnected cyber-physical bricks which will allow for the design of advanced and innovative services, and other serious games. Increasingly autonomous vehicles (UAV, UGV ...) and systems are becoming part of our daily world and can offer novel civilian applications (gaming "drones", aerial photography, vacuum cleaners ...).
- To foster the new application domain developed by the team on Software Defined Networking, the team co-organized the SDN Days (GdR CNRS RESCOM) in Loria (Nancy)

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. Software and Platforms

5.1. SecSIP

Participants: Abdelkader Lahmadi [contact], Olivier Festor.

SecSip [1] is developed by the team to defend SIP-based (The Session Initiation Protocol) services from known vulnerabilities. It presents a proactive point of defense between a SIP-based network of devices (servers, proxies, user agents) and the open Internet. Therefore, all SIP traffic is inspected and analyzed against authored Veto specification before it is forwarded to these devices. When initializing, the SecSIP runtime starts loading and parsing authored VeTo blocks to identify different variables, event patterns, operations and actions from each rule. Veto is a generic declarative language for attack patterns specification. SecSIP implements an input and output layer, to capture, inject, send and receive SIP packets from and to the network. Intercepted packets are moved to the SIP Packet parser module. The main function of this module is to extract different fields within a SIP message and trigger events specified within the definition blocks. During each execution cycle when a SIP message arrives, the SecSIP runtime uses a data flow acyclic graph network to find definition matching rules and triggers defined events. The paired events in each operator node are propagated over the graph until a pattern is satisfied. When the pattern is satisfied, the respective rule is fired and the set of actions is executed.

5.2. NDPMon

Participants: Isabelle Chrisment, Olivier Festor [contact].

The Neighbor Discovery Protocol Monitor (NDPMon) is an IPv6 implemention of the well-known ArpWatch tool. NDPMon monitors the pairing between IPv6 and Ethernet addresses (NDP activities: new station, changed Ethernet address, flip flop...). NDPMon also detects attacks on the NDP protocol, as defined in RFC 3756 (bogon, fake Router Advertisements...). New attacks based on the Neighbor Discovery Protocol and Address Auto-configuration (RFC 2461 and RFC 2462) have been identified and integrated in the tool. An XML file describes the default behavior of the network, with the authorized routers and prefixes, and a second XML document containing the neighbors database is used. This second file can be filled during a learning phase. All NDP activities are logged in the syslog utility, and so the attacks, but these ones are also reported by mail to the administrator. Finally, NDPMon can detect stack vulnerabilities, like the assignment of an Ethernet broadcast address on an interface.

[1] http://secsip.gforge.inria.fr/doku.php

NDPMon comes along with a WEB interface acting as a GUI to display the informations gathered by the tool, and give an overview of all alerts and reports. Thanks to color codes, the WEB interface makes possible for the administrator to have an history of what happened on his network and identify quickly problems. All the XML files used or produced by the daemon (neighbor cache, configuration file and alerts list) are translated in HTML via XSL for better readability. A statistic module is also integrated and gives informations about the discovery of the nodes and their type (MAC manufacturer distribution ...).

The software package and its source code is freely distributed under an opensource license (LGPL). It is implemented in C, and is available through a SourceForge project at http://ndpmon.sf.net. An open source community is now established for the tool which has distributions for several Operating Systems (Linux, FreeBSD, OpenBSD, NetBSD and Mac OS X). It is also integrated in FreeBSD ports [2]. Binary distributions are also available for .deb and .rpm based Linux flavors.

5.3. AA4MM

Participants: Laurent Ciarletta [contact], Yannick Presse.

Vincent Chevrier (MAIA team, contact), and Benjamin Camus and Julien Vaubourg (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 [49] and written in Java. This version is currently being put into APP (Agence pour la protection des programmes).

This year, we have used this software in a strategic action with EDF R&D in the context of the simulation of smart-grids. Julien Vaubourg started a PhD on this project that is co-directed by Laurent Ciarletta and Vincent Chevrier.

5.4. MASDYNE

Participant: Laurent Ciarletta [contact].

This work was undertaken in a joint PhD Thesis between MAIA and Madynes Team. Vincent Chevrier (MAIA team, LORIA) has been director and co-advisor of this PhD and is correspondant for this software, which has been used by Tomas Navarrete (MAIA team, LORIA). Other contributors to this software were: Julien Siebert, Tom Leclerc, François Klein, Christophe Torin, Marcel Lamenu, Guillaume Favre and Amir Toly.

MASDYNE (Multi-Agent Simulator of DYnamic Networks usErs) is a multi-agent simulator for modeling and simulating users behaviors in mobile ad hoc network. This software is part of joint work with the MAIA team, as part as a modeling and simulation of ubiquitous networks effort.

6. New Results

6.1. Android Security

Participants: Olivier Festor, Abdelkader Lahmadi [contact], Eric Finickel.

Android-based devices include smart phones and tablets that are now widely adopted by users because they offer a huge set of services via a wide range of access networks (WiFi, GPRS/EDGE, 3G/4G). Android provides the core platform for developing and running applications. Those applications are available to the users over numerous online marketplaces. These applications are posted by developers, with little or no review process in place, leaving the market self-regulated by users. This policy generates a side-effect where users are becoming targets of different malicious applications which the goal is to steal their private information, collect all kind of sensitive data via sensors or abusing granted permissions to make surtaxed calls or messages. To address this security issue, monitoring the behaviour of running applications is a key technique enabling the identification of malicious activities.

[2] http://www.freebsd.org/cgi/cvsweb.cgi/ports/net-mgmt/ndpmon/

During 2013, we have designed and extended a monitoring framework integrating observed network and system activities of running Android applications. We extended and enhanced our modular NetFlow probe [48] running on android devices to export observed network flow records to a collection point for their processing and analysis. Our embedded probe includes a new set of IPFIX information elements that we have designed [41] to encapsulate geographic location information within exported flows. This work was done in collaboration with the Univerisity of Twente, where they developed the flow collector and the analysis application.

We have also developed an embedded logging probe that exports available logs generated by an Android device to a big data enabled store [25]. We have analyzed the collected logs using TreeMapping visualization technique [46] to display behavioral graphs of Android applications. The generated graphs are able to provide an aggregated view of the different components of a running application. This view is useful to improve the understanding of the behaviour of an application.

6.2. Sensor networks monitoring

Participants: Rémi Badonnel, Alexandre Boeglin, Isabelle Chrisment, Olivier Festor, Abdelkader Lahmadi [contact], Anthea Mayzaud, Bilel Saadallah.

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. They are dynamic and the connectivity is limited and fluctuant over time. Each node may loss frequently its connectivity with its neighborhood nodes. In addition, link layer frames have high constrains on their size and throughput is limited. These networks are used for many different applications including industrial automation, smart metering, environmental monitoring, homeland security, weather and climate analysis and prediction. The main issue in those networks is optimal operation combined with strong energy preservation. Monitoring, i.e the process of measuring sampled properties of nodes and links in a network, is a key technique in operational LLNs where devices need to be constantly or temporally monitored to assure their functioning and detect relevant problems which will result in an alarm being for- warded to the enterprise network for analysis and remediation.

We developed and designed a novel algorithm and a supporting framework [16] that improves a distributed poller-pollee based monitoring architecture. We empower the poller-pollee placement decision process and operation by exploiting available routing data to monitor nodes status. In addition, monitoring data is efficiently embedded in any messages flowing through the network, drastically reducing monitoring overhead. Our approach is validated through both simulation, implementation and deployment on a 6LoWPAN-enabled network. Results demonstrate that our approach is less aggressive and less resource consuming than its competitors.

In a previous work, we developed a first fully operational content centric networking protocol stack (CCNx) dedicated to a wireless sensor network. During this year, we have extended this implementation and designed a novel monitoring service [32] to efficiently aggregate data in a WSN. The developed solution has been implemented in the Contiki operating system and evaluated using the Cooja simulator. We have compared the performance of our proposed solution with the SPIN protocol in terms of the number of exchanged messages and response times. Our results show that our solution provides better performance for collecting and aggregating data inside the network using operators such as maximum or average.

This year, we also analyzed security attacks against LLN networks, and more specifically those targeting the RPL routing protocol. In that context, we introduced a taxonomy in order to classify these attacks into three main categories. The attacks against resources, such as DIS flooding attacks and increased rank attacks, permit to reduce the network lifetime through the generation of fake control messages or the building of RPL loops. The attacks against the topology, such as wormhole attacks or DAO inconsistency attacks, permit the network to converge to a sub-optimal configuration or to isolate one or several nodes. Finally, attacks against network traffic, such as eaves-dropping attacks and decreased rank attacks, permit to capture and analyse large part of the RPL traffic.

Based on this taxonomy, we compared the properties of attacks and discussed methods and techniques for monitoring them. In particular, we are investigating efficient solutions for supporting security monitoring in these resource-constrained environments [17]. We considered DODAG inconsistency attacks as a first case study. Scenarios were constructed to evaluate the performance of the RPL network when such attacks are carried out. Via an implementation in Contiki, it was identified that the internal mechanism proposed by RPL, which involves ignoring packets with the appropriate IPv6 header after a fixed threshold is reached, uses an arbitrary value for the threshold. A new function that dynamically scales this threshold was developed to improve performance of the network while under attack. In addition, a comparative study between the (1) no threshold, (2) fixed threshold and (3) dynamic threshold scenarios has been performed.

6.3. Monitoring of anonymous networks

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

Anonymous networks have emerged to protect the privacy of network users and to secure the data exchange over the Internet. Nevertheless, the monitoring of these networks has not been investigated very much and only few networks have been studied. Large scale monitoring on these systems allows us to understand how they behave and which type of data which is shared among users.

In 2013, we continued our research about anonymous systems, with a special focus on the I2P network [3]. The I2P network provides an abstraction layer to permit two parties to communicate in an anonymous and secure manner. This network is optimized for anonymous web hosting and anonymous file-sharing. I2P's file-sharing community is highly active, where users deploy 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.

Current statistics service for the I2P network do not provide values about the type of applications deployed in the network nor the geographical localization of users. We conducted the first large-sale monitoring on the I2P anonymous system, characterizing users and services running on top of the network. We first designed and implemented a distributed monitoring architecture based on probes placed in the I2P's distributed hash table (I2P's netDB), which allows us to collect a vast amount of network metadata. So, our distributed monitoring architecture provides us with different insights about the I2P network.

We were able to detect the behavior of particular applications, notably their period of activity. By considering the behavior of a particular anonymous service along with a particular set of I2P users, we determined in which measure this set of users was responsible for the activity of the anonymous service. We thus conducted a correlation analysis between the behavior of I2P users from two top cities along with the behavior of anonymous file-sharing clients (I2PSnark clients) throughout a particular period of time. By applying Pearson's correlation coefficient, we achieved a group-based characterization and we determined that the activity of users from those cities explained 38% of all detected file-sharing activity [22], [2].

Starting from our limitations to de-anonymise a particular I2P user, we studied I2P's unidirectional tunnels and the mechanism used to create these tunnels. We discovered a vulnerability in this mechanism, vulnerability which allows an attacker to detect whether a user is the last participant in an inbound tunnel. With this knowledge, we showed that it would be possible to attack an I2P's eepsite in order to de-anonymise the eepsite's operator [39].

6.4. Configuration security automation

Participants: Rémi Badonnel [contact], Martin Barrere, Olivier Festor.

The main research challenge addressed in this work is focused on enabling configuration security automation in autonomic networks and services. In particular our objective is to increase vulnerability awareness in the autonomic management plane in order to prevent configuration vulnerabilities. The continuous growth of networking significantly increases the complexity of management. It requires autonomic networks and services that are capable of taking in charge their own management by optimizing their parameters, adapting their configurations and ensuring their protection against security attacks. However, the operations and changes executed during these self-management activities may generate vulnerable configurations.

[3] http://i2p2.de

A first part of our work in the year 2013 has been dedicated to the issue of past hidden vulnerable states [8]. Even though a known vulnerability may not be present on a current system, it could have been unknowingly active in the past providing an entry point for attacks that may still constitute a potential security threat in the present. Indeed, vulnerabilities can survive within active systems for a long period of time without being known. During this period, attackers may perform well-planned and clean attacks (e.g., stealing information) without being noticed by security entities (e.g., system administrators, intrusion detection systems, self-protection modules). Changes on the system or even its normal activity can alter or erase the remaining evidence on the current configuration. In that context, we have defined a new strategy for assessing past hidden vulnerable states. This solution is based on a mathematical model for describing and detecting unknown past security exposures and on an OVAL-based framework able to autonomously build and monitor the evolution of network devices and to outsource the assessment of their exposure in an automatic manner. We also have developed an implementation prototype that efficiently performs assessment activities over an SVN repository of IOS system images. Experimental results have confirmed the feasibility and scalability of our solution.

A second part aimed at light-weighting the vulnerability assessment process in the context of mobile devices [9]. Security activities imply a consumption of resources that should be taken to a minimum in order to maximize the performance and responsiveness of such critical environments. Sometimes users may prefer to deactivate security processes such as antivirus software instead of having a short battery lifetime. The proposed approach centralizes main logistic vulnerability assessment aspects as a service while mobile clients only need to provide the server with required data to analyze known vulnerabilities described with the OVAL language. By configuring the analysis frequency as well as the percentage of vulnerabilities to evaluate at each security assessment, our probabilistic solution permits to bound client resource allocation and also to outsource the assessment process. The strategy consists in distributing evaluation activities across time thus alleviating the workload on mobile devices, and simultaneously ensuring a complete and accurate coverage of the vulnerability dataset. This technique results in a faster assessment process, typically done in the cloud, and considerably reduces the resource allocation on the client side. A prototype of our vulnerability assessment framework for Android has been selected and presented during the demonstration session of the IEEE/IFIP IM'2013 international conference [10].

We are currently investigating new methods for remediating known vulnerabilities, formalizing the change decision problem as a satisfiability or SAT problem [27]. By specifying our vulnerability knowledge source as a logical formula, fixing those system properties we can not change and freeing those variables for which changes are available, our objective is to use a SAT solving engine for determining what changes have to be made so as to secure the system. In order to provide proactive and reactive solutions, we are interested in the concept of future state descriptions to specify how a system will look like after applying a specific change.

6.5. Cache Management in CCN

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

The Internet is currently mostly used for accessing content. Indeed, ranging from P2P file sharing to current video streaming services such as Youtube, it is expected that content will count for approximately 86% of the global consumer traffic by 2016.

While the Internet was designed for -and still focuses on- host-to-host communication (IP), users are only interested in actual content rather than source location. Hence, new Information-Centric Networking architectures (ICN) such as CCN, NetInf, Pursuit have been proposed giving high priority to efficient content distribution at large scale. Among all these new architectures, Content Centric Networking (CCN) has attracted considerable attention from the research community [4].

CCN is a network architecture based on named data where a packet address names content, not location. The notion of host as defined into IP does not exist anymore. In CCN, the content is not retrieved from a dedicated server, as it is the case for the current Internet. The premise is that content delivery can be enhanced by including per-node-caching as content traverses the network. Content is therefore replicated and located at different points of the network, increasing availability for incoming requests.

[4] http://www.ccnx.org

As content is cached along the path, it is crucial to investigate the caching strategy for CCN Networks and to propose new schemes adapted to CCN. We therefore designed *Most Popular Content* (MPC), a new caching strategy for CCN network [12], [11].

Instead of storing all the content at every nodes on the path, MPC strategy caches only popular content. With MPC, each node counts all the requests for a content and when it has been requested a large amount of time, the content will be cached at each node along the path. Otherwise, the content is not popular; it is transmitted but it is not cached into the network.

We implemented MPC into the ccnSim simulator and evaluate it through extensive simulations.

Our results demonstrate that using MPC strategy allow to achieve a higher Cache Hit in CCN networks and still reduces drastically the number of replicas. By caching only popular content, MPC helps at reducing the cache load at each node and the network resource consumption.

We expect that our strategy could serve as a base for studying name-based routing protocols. Being a suggestion based mechanism, it is feasible to adapt it to manage content among nodes, to predict popularity and to route content to destination. In addition, we are currently investigating the social relationship between users to improve our caching strategy for CCN networks.

Besides, Online Social Networks (OSN) have gained tremendous popularity on the Internet. Millions of users interact with each other through OSN such as Facebook or Twitter. New ubiquitous devices (smartphones, tablets) appeared and include functionalities to instantaneously share information through OSN. As a central component of CCN is in-network caching, the content's availability depends on several criteria such as cache strategies and replacement policies, cache size or content popularity. OSN carry extremely valuable information about users and their relationships. This knowledge can help to drastically improve the efficiency of Content Centric Networks. Thus, we propose to include social information in the design of a new caching strategy for Content Centric Networking. We designed *SACS*, a novel caching strategy for CCN based on the social information of users [28]. Our socially-aware caching strategy gives priority to content issued by Influential users and cache it pro-actively into the CCN network. We performed simulations of our caching strategy and show its ability to improve the cache performances of CCN. In addition, we implemented a prototype on PlanetLab and performed large-scale experiments. Our solution improves the caching performances of CCN by 2.5 times on real testbed.

6.6. QoS in Wireless Sensor Networks

Participants: François Despaux, Abdelkader Lahmadi, Evangelia Tsiontsiou, Kévin Roussel, Moutie Chehaider, 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, but also high throughput with self-adaptation to dynamic traffic changes. Our research on WSN QoS is thoroughly organized in four topics:

- self-adaptive MAC protocol for both QoS and energy efficiency

  By combining our two previous MAC protocols called Queue-MAC and CoSenS, we extended Queue-MAC to iQueue-MAC to support multi-hop transmission [23], [6]. iQueue-MAC provides immediate yet energy-efficient throughput enhancement for dealing with burst or heavy traffic. Combined with CSMA/CA, iQueue-MAC makes use of queue length of each sensor node and allocates suitable TDMA slots to them for packets transmission. During light traffic period, no extra slots will be allocated; iQueue-MAC acts like other low duty-cycle MACs to conserve power. While in burst or heavy traffic period, iQueue-MAC senses the build up of packet queues and dynamically schedules adequate number of slots for packet transmission. Within ANR QUASIMODO project, we have implemented iQueue-MAC on STM32W108 chips that offer IEEE 802.15.4 standard communication. We set up several real-world experimental scenarios, including a 46 nodes multi-hop test-bed for simulating a general application, and conducted numerous experiments to evaluate iQueue-MAC, in comparison with other traffic adaptive duty-cycle protocols, such as multi- channel

version RI-MAC and CoSenS. Results clearly show that iQueue-MAC outperforms multi-channel version of RI-MAC and CoSenS in terms of packet delay and throughput.

- QoS routing

  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. In practice, the complexity of the existing routing algorithms is too high to be implemented on the low cost and power constrained sensor nodes. Recently, Operator calculus (OC) has been developed by Schott and Staples with whom we collaborate. OC can be applied to solving MCOP problem with lower complexity and can deal with dynamic topology changes (which is the case in duty-cycled WSN). Through intensive numerical experiments, we have shown that OC has much less complexity compared with SAMCRA, known as one of the best existing algorithms. Sub-optimal paths can be obtained with a distributed version of OC, and following this principle, a first OC-based routing protocol is implemented over Contiki rime stack on TelosB motes. Its improvement and performance evaluation, as well as its integration to uIP/RPL stack is our ongoing work.
- Systems and middleware for supporting QoS in wireless sensor networks

  For supporting new protocols implementation which require to interact with low level services (MAC, Radio drivers, hardware timers) and integration to the Internet of Things approach, we focused on the OS for WSN. Several contributions have been made available for both ContikiOS (https://github.com/contiki-os/contiki/pull/519) and RiotOS (https://github.com/RIOT-OS/RIOT/pull/408, https://github.com/RIOT-OS/RIOT/pull/459). This allows to preparing for the next step towards the implementation of iQueue-MAC on both ContikiOS and RiotOS and compare experimentally with other protocols. In parallel and as part of LAR project, we also investigated the integration of different types of WSN using a gateway to make the data access transparent following RESTful webservice through CoAP/UPD/6loWPAN [24].
- End-to-end performance in multi-hop networks

  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 slotted CSMA/CA (beacon enabled mode of IEEE 802.15.4). One of the problem of the existing 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 [15], [14]. We proposed to explore a new approach which is based on process mining to extract the Markov chain model from the execution of the protocol code.

6.7. Routing in Wireless Sensor Networks

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

Our work on the estimation of the remaining energy inside a sensor is published in [18]. We have integrated this model in the standard routing protocol for wireless sensors networks (RPL) and compared our energy based routing against a routing plane based on the quality of transmission between sensors [30].

We have built a new model to combine together several criteria, as the remaining energy, the expected transmission rate and the hop count into one quality indicator. To achieve this, we propose to use fuzzy logic either because it is a recognized mathematical tool for combining heterogeneous data and because it can be implemented with a small memory footprint. Our work is fully integrated in the standard protocol and does not need additional messages or new protocol states.

We bought 35 sensors and deployed them in the Loria building. The goal of this deployment is manyfold :

- to build and observe a real network in a real environment;
- to provide the team with a demonstrative tool to help the understanding of our work;
- to provide the team with a testbed for other works on IoT, like the security monitoring or the QoS.

6.8. Online Risk Management

Participants: Rémi Badonnel [contact], Oussema Dabbebi, Olivier Festor.

Telephony over IP has known a large scale deployment and has been supported by the standardization of dedicated signaling protocols. This service is however exposed to multiple attacks due to a lower confinement in comparison to traditional PSTN networks. While a large variety of methods and techniques has been proposed for protecting VoIP networks, their activation may seriously impact on the quality of such a critical service. Risk management provides new opportunities for addressing this challenge. In particular our work aims at performing online risk management for VoIP networks and services. The objective is to dynamically adapt the service exposure with respect to the threat potentiality, while maintaining a low security overhead.

In the year 2013, these efforts on VoIP risk management have led the PhD defense of Oussema Dabbebi. This work has been structured into three axes [1]. The first axis concerns the automation of the risk management process in VoIP enterprise network. In this context, we have developed a mathematical model for assessing risk, a set of progressive countermeasures to counter attackers and mitigation algorithms that evaluate the risk level and takes the decision to activate a subset of countermeasures [4]. To improve our strategy, we have coupled it with an anomaly detection system based on SVM and a self-configuration mechanism which provides feedback about countermeasure efficiency. The second axis deals with the extension of our adaptive risk strategy to P2PSIP infrastructures. We have implemented a specific risk model and a dedicated set of countermeasures with respect to its peer-to-peer nature. For that, we have identified attack sources and established different threat scenarios. We have analysed the RELOAD framework and proposed trust mechanisms to address its residual attacks. Finally, the third axis focuses on VoIP services in the cloud where we have proposed a risk strategy and several strategies to deploy and apply countermeasures [5].

6.9. Pervasive Computing

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

Vincent Chevrier, Thomas Navarrete Gutierrez and Julien Vaubourg (MAIA team) did contribute to part of this activity.

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. In a related field, Cyber Physical Systems also are technological systems that have to be considered within a physical world and its contraints. They are complex systems where several inter-related phenomena have to be considered. In order to be studied, modeled and evaluated, we propose the use of co-simulation and multimodeling.

Pervasive Computing is about interconnected and situated computing resources providing us(ers) with contextual services. 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're applying this work on UAvs, dynamic networks (adhoc, mesh, P2P, wireless sensors and actuators), energy-constrained / location aware services, smart grids etc.

Such systems can be seen as complex and are present everywhere in our environment: internet, electricity distribution networks, transport networks. This systems have as characteristics: a large number of autonomous entities, dynamic structures, different time and space scales and emergent phenomena.

Application domains such as Smart Spaces, Smart Cities, Smart Trasportation Systems and Smart Grid makes us sometimes use Smart* or SmartX as a generic word. Madynes is focusing on the networking aspects of such systems and on the tools to develop and assess them. We cooperate with other teams and most notably the Maia team to be able to encompass issues and research questions that combine both networking and cognitive aspects.

In 2013 we worked on the following research topics :

- Assessment and evaluation of complex systems. Continuing the work on multi-modeling and co-simulation, we have participated with the MAIA team on the development of an architecture for the control of complex systems based on multi-agent simulation, a CPS co-simulation (next item) and a Smart grid simulation tool (last item), and continue working on the AA4MM framework (Agents and artefacts for Multiple heterogeneous Models).

  A control architecture has been proposed by Tomas Navarrete, based on an “equation-free” approach. We use a multi-agent model to evaluate the global impact of local control actions before applying the most pertinent set of actions. 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 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. We have also executed experiments with different configurations of the architecture to identify the different means to improve the performance of the architecture.

  This work helped us to identify [13] the key issues related to the usage of the multi-agent paradigm in the context of control of complex systems.

- In Cyper Physical Systems, we have lead the design and implementation of the Aetournos (Airborne Embedded auTonomOUs Robust Network of Objects and Sensors) platform at Loria. The idea of AETOURNOS is to build a platform which can be at the same time a demonstrator of scientific realizations and an evaluation environment for research works of various teams of our laboratory. It is also its own research domain : building a completely autonomous and robust flock of collaborating UAVs.

  In Madynes, we focus on the CPS and their networks and applications. Those systems consist of numerous autonomous elements in sharp interaction which functioning require a tight coupling between software implementations and technical devices. The collective movements of a flock of flying communicating robots / UAVs, evolving in potentially perturbed environment constitute a good example of such a system. Indeed, if we look at the level of each of the elements playing a role into this system, a certain number of challenges and scientific questions can be studied: respect of real-time constraints of calculations for every autonomous UAV and for the communication between the robots, conception of individual, embedded, distributed or global management systems, development of self-adaptative mechanisms, conception of algorithms of collective movement etc... Furthermore, the answers to each of these questions have to finally contribute to the global functioning of the system. Applying co-simulation technique we plan to develop a hybrid "network-aware flocking behavior" / "behavior aware routing protocol". The platform is composed of several high-grade research UAVs (Pelican quadcopters and Firefly hexacopters) and lighter models (AR.Drone quacopters). 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.

  This work is discribed in a position paper where a first implementation of a formation flight is detailed [29].

- Smart grids and Smart spaces are another application domain. MS4SG (cf. 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’ve so far successfully applied

our solution to the simulation of smart appartment complex and to combining the electrical and networking part of a Smart Grid (first deliverable and first workshop with EDF R&D, Supélec and SIANI were in september 2013). A paper has also been accepted to Simutools 2014. In 2014, 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* [13].

6.10. SCADA Systems Security

Participants: Olivier Festor, Abdelkader Lahmadi [contact], Bilel Saadallah.

SCADA is a term used in several industries and it 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 including: power generation and distribution, transportation, nuclear plants, manufacturing processes, etc. SCADA systems use a family of network protocols (PROFINET, MODBUS, DNP3) to monitor and control these industrial activities or even our homes. SCADA systems are 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. Several of them are daily discovered and disclosed or remain still unknown. The most threaten accidents in SCADA networks are caused by targeted attacks, where adversaries exploit those vulnerabilities available in software or network protocols components to disturb and make damage to the physical process. Therefore, it is important to provide new methods and tools for protecting SCADA network from malicious cyber attacks targeting physical processes and infrastructures.

During the year 2013, we have firstly designed and setup a SCADA test bed [31] to be able to analyze and develop security methods for several controlled physical systems. The testbed uses a Profinet based network to control experimental real-time simulated physical processes through hardware programmable logic controllers (PLCs). Secondly, we have developed a novel methodology to automatically discover a pattern of behaviour of a running controlled system through the analysis of communication messages traveling in its control loop network. The method applies process mining techniques on the exchanged communication packets between control and feedback devices to infer a model of the controlled running system. The extracted model will be then used to build a tailored anomaly-based intrusion detection module for the studied system.

6.11. Dynamic resource allocation for network virtualization

Participants: Said Seddiki, Bilel Nefzi, Mounir Frikha, 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. Sharing resources and improving utilization are the main idea of virtualization. Finding effective solutions for the needs expressed by users without deteriorating the performance of different VNs is a research challenge. In addition, solutions should meet different performance criteria required by network infrastructure.

We proposed several approaches that aim to select substrate nodes [21] with sufficient CPU, disk, and other resources, as well as substrate links with enough spare bandwidth [19], [20]. These dynamic approaches, where online monitoring of the VN is required, allow adaptively changing the resource allocations. We have shown through simulations that the proposed approaches offer higher utilization of physical network and better managing the satisfaction of virtual networks by minimizing the packet delays inside the physical node. They also provide a fair and efficient allocation of link capacity and avoid bottlenecks. The next step is the implementation of these propositions using OPENFLOW in a software defined network.

6.12. Crowdsourcing Services

Participants: Thomas Silverston [contact], Olivier Festor, Abdelkader Lahmadi, Elian Aubry.

Nowadays cities invest more in their public services, and particularly digital ones, to improve their resident's quality of life and attract more people. Thus, new crowdsourcing services appear and they are based on contributions made by mobile users equipped with smartphones. For example, the respect of the traffic code is essential to ensure citizens' security and welfare in their city. We therefore designed CrowdOut, a new mobile crowdsourcing service for improving road safety in cities. CrowdOut allows users to report traffic offense they witness in real time and to map them on a city plan. CrowdOut has been implemented and experiments and demonstrations have been performed in the urban environment of the Grand Nancy, in France. This service allows users appropriating their urban environment with an active participation regarding the collectivity. This service also represents a tool for city administrators to help for decisions and improve their urbanization policy, or to check the impact of their policy in the city environment.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry: Inria-EDF Strategic action MS4SG

Participants: Laurent Ciarletta, Yannick Presse.

Vincent Chevrier and Julien Vaubourg (MAIA team, LORIA) are external collaborators.

The MS4SG (multi-simulation for smart grids) project is part of a strategic action between Inria and EDF. It is a joint work between the Madynes and MAIA teams from Inria-NGEt 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.

Smart grids are energy power grids (electricity) endowed with smart capabilities because of the use of information and communication technologies. It 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. In Smart-grids, power/electricity utilities and distributors have to deal with multiple and variable sources of energy and of errors, the mandatory integration of smaller energy providers and a very variable set of users, while maintaining the necessary quality of service. All this at a scale than can be as big as a country. The IT+Network layers add the needed « smart » to allow dynamic adaptation of the different components and help forecast and therefore pilot the entire system. Smart grids correspond to new challenges because it is needed to re-think the way electricity is supplied to customers.

The idea behind MS4SG is to use simulation to help develop and evaluate future 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 following initial different domains: electrical networks, communication networks and information systems. 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). In addition, each domain has developed is own set of software that should ideally be reused.

8. Partnerships and Cooperations

8.1. Regional Initiatives

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 AAL 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 and IoT technology.

8.2. National Initiatives

8.2.1. ANR

8.2.1.1. ANR Quasimodo

Participants: François Despaux, Abdelkader Lahmadi, Evangelia Tsiontsiou, 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 for duration of 36 months. 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). We extended queue-MAC to iQueue-MAC to support multi-hop transmission [23]. We also conducted measurement based performance evaluation of IEEE802.15.4 beacon enabled WSN to assess the usefulness of the existing Markov models [15], [14] for evaluating the end-to-end delay distribution. A new routing algorithm called Operator calculus has been intensively studied and its execution time has been compared with SAMCRA, showing the great potential of OC to be used in WSN routing.

8.2.2. PIA 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 assistive 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. The first step consists in identifying and developing necessary support for realizing such a system. For this purpose we investigated several OS for WSN and proposed some enhancements to ContikiMAC and RiotOS.

8.2.3. Action de Développement Technologique

8.2.3.1. ADT Métroscope

This ADT is linked to the consortium Metroscope [5], 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 will participate in the design and deployment of a distributed platform. This platform will be composed of a services providing measurement tools that collect a set of data and interact with probes located at various points of the network.

8.2.3.2. 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.

8.2.3.3. ADT PAL-PERCEE

The goal of this ADT (2012-2013) is to provide a multi-protocol gateway and a unified interface for easing transparent access to the heterogenous sensor data. Together with PAL partners, we specified a common data format and enriched the existing MPIGate by re-structing all using ROS middleware. The new MPIGate is operational in the smart apartment of LORIA and serves as the base for developing large scale AAL systems.

[5] http://metroscope.eu/

8.2.4. Actions d'Envergure Nationale

The Inria Large-scale initiative action AEN 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 and thanks to the associated ADT PERCEE project described above, we extended MPIGate (http://mpigate.loria.fr). The development and tests are conducted using LORIA's smart apartment platform developed within CPER MISN Informatique située project (http://infositu.loria.fr). The adoption of ROS (Robotic Operating System) 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 Projects

8.3.1.1. Univerself

Type: COOPERATION

Defi: The Network of the Future

Instrument: Integrated Project

Objectif: The Network of the Future

Duration: September 2010 - August 2013

Coordinator: Alcatel Lucent (France)

Partner: Universiteit Twente, Alcatel Lucent Ireland, Alcatel Lucent Deutschland, Valtion Teknillinen Tutkimuskeskus (Finland), University of Piraeus, France Telecom, Telecom Italia, National University of Athens, Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung, Interdisciplinary Institute for Broadband Technology, Telefonica Investigacion y Desarrollo, Thales Communications, Inria, Nec Europe, University of Surrey, University College London, IBBT (Belgium).

Inria contact: E. Fabre

See also: http://www.univerself-project.eu/

Abstract: UniverSelf unites 17 partners with the aim of overcoming the growing management complexity of future networking systems, and to reduce the barriers that complexity and ossification pose to further growth. Univerself has been launched in October 2010 and is scheduled for four years.

This FP7 European integrated project aims at consolidating the autonomic methods and techniques supporting the management of the future Internet, and at integrating these methods into a unified management framework (UMF). The objective of this framework is to address the management issues of the evolving Internet through the self-organization of the control plane and the empowerment of the management plane with cognition. Our work in the Univerself project mainly concerns the security and safety challenges posed by this unified management framework, with a special interest for the maintenance of safe configurations.

In the Year 2013, we have pursued our efforts on vulnerability management in autonomic networks and systems. In that context, we have worked on the adaptation of observation and operation methods to the specific needs of future networks and services, through the refinement of the Unified Management Framework (UMF) and its network empowerment modules (NEM). A particular focus has been given to methods for assessing past hidden vulnerable configurations [44] as well as techniques for minimizing the impact of the vulnerability assessment process on device resources [45]. We have therefore extended our vulnerability management strategy to the detection of systems compromised in the past by configuration vulnerabilities unknown at that moment, and considered a probabilistic cost-efficient assessment for dealing with resource-constrained environments by taking advantage of the statistical properties of vulnerability description sets.

We have also worked on the design of a configuration assessment service for the UMF framework. NEMs have particular requirements and specific configurations in order to work properly. The interconnections between hundreds of NEMs and the services provided by them increase the complexity of their configuration. This configuration assessment service aims at preventing configuration errors, conflicts between services and inconsistencies that can occur leading to severe operational problems as well as security issues within the framework itself. Even though operating systems where NEMs are deployed and also the NEMs themselves may have security solutions to be protected, such fact does not ensure the security of the whole framework.

8.3.1.2. FI-WARE

Type: COOPERATION

Defi: PPP FI: Technology Foundation: Future Internet Core Platform

Instrument: Integrated Project

Objectif: PPP FI: Technology Foundation:Future Internet Core Platform

Duration: September 2011 - May 2014

Coordinator: Telefonica (Spain)

Partner: 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. FI-WARE is designed to meet the demands of key market stakeholders across many different sectors, e.g., healthcare, telecommunications, and environmental services. FI-WARE unites major European industrial actors.

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 in earlier research projects. We will demonstrate how this infrastructure supports emerging Future Internet (FI) services in multiple Usage Areas, and will exhibit significant and quantifiable improvements in the productivity, reliability and cost of service development and delivery, building a true foundation for the Future Internet.

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. More specifically, the tool uses the Scapy library for packet manipulation, allows users to define interaction scenarios in XML and provides multiple mutation algorithms;
- 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.

8.3.1.3. Flamingo

Type: COOPERATION

Defi: Management of the Future Internet

Instrument: Network of Excellence

Objectif: Management of the Future Internet

Duration: November 2012 - October 2016

Coordinator: University of Twente (Netherlands)

Partner: 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 [40].

Our work on network and service monitoring [42] has focused on security attacks in RPL Networks, with a study of DODAG inconsistency attacks jointly with Jacobs University of Bremen. In a RPL network, a malicious node can create artificial DODAG inconsistencies by manipulating IPv6 header options, thereby leading to increased overhead, denial of service and even black-hole attacks that are hard to detect. Our work has consisted in evaluating the impact of DODAG attacks in a RPL network, identifying the key parameters that are required to detect these attacks, developing a mitigation strategy to reduce their effects. Efforts have also been done on a NetFlow/IPFIX Probe for android-based devices, jointly with University of Twente. The major achievements of this collaboration have been the development of a NetFlow and IPFIX metering process for Android devices, the extension of nfdump/Nfsen and SURFmap with location support, and a IETF draft describing a set of information elements for IPFIX metering process location.

We have also contributed to activities on automated configuration and repair [37], with an in-depth analysis and comparison of existing management architectures. In that context, we have elaborated a survey on autonomic vulnerability assessment, recently published in IEEE Communications Survey and Tutorial [3]. This survey introduces a classification, called D3, to structure the vulnerability assessment activity into three well-defined dimensions: Discovery, Description and Detection. Background and key concepts as well as different leading methods and current techniques have been discussed along this work. We have identified potential applications over diverse contributions that may provide a strong basis for achieving this critical goal within self-governing systems. We have also pointed out several areas such as vulnerability integration models, collaborative vulnerability management approaches and policy-based reasoning systems where the development of novel approaches and solutions are required to provide autonomic environments with the ability of assessing their own exposure.

8.3.2. Collaborations in European Programs, except FP7

Type: COOPERATION

Defi: Crowdsourcing Services for Citizen in Digital Cities

Instrument: EIT ICT Labs

Objectif: Develop new essential services for city-grade crowd-sourcing platforms and to deploy them on different platforms dedicated to different types of crowd-sourcing activities.

Duration: January 2013 - December 2013

Coordinator: Inria (France)

Partner: Imperial College of London (UK), BME (HU), KTH (SW), SAP (GE), Cap-Digital (FR), Alcatel-Luccent (FR), Inria (FR)

Inria contact: Thomas Silverston

See also: http://www.eitictlabs.eu

Abstract: the EIT ICT Labs activity CityCrowdSource is composed of 7 partners, among which 4 partner universities and 3 partner industries. This project tackles the Crowdsourcing services and propose three milestones for such emerging services: trust service, privacy service and process model.

The objective of CityCrowdSource is to develop three new services that are essential for city-grade crowd-sourcing platforms and to deploy and evaluate them on five different existing platforms dedicated to different types of crowd-sourcing activities.

The activity supports to leverage the potential of crowd-based applications in urban contexts. Crowd-based data collection in combination with official data will lead to a vastly improved coverage and quality of digital information for urban areas.The added-value of the proposal is in : (1) the three services: trust, privacy and crowd processes modeling that are not present in any crowd-sourcing platform available today, (2) in the deployment and of these services on top of different crowd-sorucing platforms and (3) the experimentation of these paltforms in real life city scenarios.

Our work in this activity has focused on the design, deployment and experimentation of CrowdOut, a crowdsourcing service for Road Safety. This service has been designed for Android platform and has been tested and evaluated. First, a prototype has been experimented during Futur-en-Seine, the Digital World Festival in Paris (June 2013). Second, we performed experiment in the Grand Nancy Urban Area. The CrowdOut User Interface received support from the Living Lab Inria Sophia-Antipolis.

From this work we published several papers into a national conference (Ubimob) [25].

8.3.3. Collaborations with Major European Organizations

University of Luxembourg (Luxembourg) : We have two ongoing PhD candidates with the SnT at University of Luxembourg. We collaborate on the topic of Large Scale Monitoring for Security Management. Target services are: P2P Networks, Virtual Coordinates Systems and DNS Services.

8.4. International Initiatives

8.4.1. Inria International Partners

8.4.1.1. 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

8.5. International Research Visitors

8.5.1. Visits of International Scientists

8.5.1.1. Internships

Younes Abid

Subject: Development of a configuration service for Wireless Sensor Networks using a content centric approach

Date: from Mar 2013 to Sep 2013

Institution: Ecole Nationale des Sciences de l'Informatique (Tunisia)

Narjess Derouiche

Monitoring of the Anonymous I2P Network

Date: from Avril 2013 to Sep 2013

Institution: Ecole supérieure des communications de Tunis (SUP'COM) (Tunisia)

Fadwa Rebhi

Subject: Development of an automated detection tool of malicious applications in Android-based smartphones

Date: from Mar 2013 to Sep 2013

Institution: Ecole Nationale des Sciences de l'Informatique (Tunisia)

Evangelia Tsiontsiou

Subject: Multi-constrained QoS routing for wireless sensor networks

Date: from March 2013 to July 2013

Institution: Université Nationale Capodistrienne d'Athènes (Greece)

Achraf Weslati

Subject: Co-Simulation applied to Networking, Driving and Pedestrian

Date: from Mar 2013 to Sep 2013

Institution: Ecole Nationale des Sciences de l'Informatique (Tunisia)

8.5.1.2. Scientific visits

Participant: Juan Caubet.

Visiting PhD student

Subject: A Distributed Authentication System for Content-Centric Networking

Date: from Aug 2013 to Nov 2013

Institution: Technical University of Catalonia (UPC) (Spain)

Visiting PhD Student Aug 2013 to Nov 2013

8.5.2. Visits to International Teams

Anthea Mayzaud visited the Jacobs University in Bremen, Germany, during August 2013, more precisely in the Computer Science department leaded by Jürgen Schönwälder. The purpose of the visit was to define the exact collaboration possible between the two research groups within the area of securing RPL networks by using risk mitigation approaches. A secondary purpose was to get familiar with the Contiki RPL implementation and the tools, such as Cooja, provided by Contiki in order to implement the chosen risk mitigation approach. A joint paper between the research group at Jacobs and Inria on the "Mitigation of RPL DAG Inconsistency Attacks by Dynamically Rate Limiting Local Repair" has been written as a result of this visit.

9. Dissemination

9.1. Scientific Animation

Abdelkaer Lahmadi served as a reviewer for the following journals: IEEE Communications Magazine, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Network and Service Management.

Abdelkader Lahmadi served as a Technical Program Committee member for the following conferences: Autonomous Infrastructure, Management and Security (AIMS'2013, PhD student workshop), The 1st International Workshop on Crowdsensing Methods, Techniques, and Applications (CROWDSENSING 2014).

Abdelkader Lahmadi participated to the Dagstuhl Seminar "Global Measurement Framework".

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.

Isabelle Chrisment is a member of AFNIC[6] 'scientific board since January 2013.

Isabelle Chrisment served as a TPC member of : the 7th International IFIP Conference on Autonomous Infrastructure, Management and Security (IFIP AIMS'2013); the 14th joint TC6 and TC11 International IFIP Conference on Communications and Multimedia Security (IFIP CMS'2013); the IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM'13); the 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2013), Security and Privacy Track. the 8th national conference on Sécurité des Architectures Réseaux et des Systèmes d'Information (SARSSI 2013).

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. In 2013, we organized four workshops leading to a new work-plan for the design of new management protocols and services within the IRTF.

Olivier Festor served as a Technical Program Committee Member of the following 2013 events:

IFIP/IEEE Integrated Management Symposium (IM'2013), IFIP/IEEE in conjunction with ACM CNSM'2013. Asia-Pacific Network Operations and Management Symposium (APNOMS'2013 and IEEE GLOBECOM 2013.

Olivier Festor is member of the board of editors of the Springer Journal of Network and Systems Management. He is member of the editorial board of the IEEE Transactions on Network and Service Management.

In December 2012, Olivier Festor joined the University of Lorraine on a Full Professor position. There he became Director of the TELECOM Nancy Engineering School (350 students at Masters level, 50 faculty and staff).

[6] http://www.afnic.fr

Remi Badonnel served as a TPC member of the following conferences:

- the IFIP International Conference on Autonomous Infrastructure, Management and Security (IFIP AIMS'2013);
- the IEEE International Conference on Integrated Management (IEEE/IFIP IM'2013);
- the IEEE/IFIP International Workshop on Management of the Future Internet (IEEE/IFIP MANFI'2013).

Remi Badonnel served as a session chair and was part of the Best Paper Award Committee at the IEEE International Conference on Integrated Management (IEEE/IFIP IM'2013).

Remi Badonnel served as an expert for the "Futur et Ruptures" programm of the Mines-Telecom institute.

Thibault Cholez was invited to present a tutorial [38] on the Management of Content-Centric Networking at ResCom 2013, a CNRS summer school .

Thomas Silverston leads in 2013 the activity CityCrowdSource from EIT ICT Labs. He also co-organized the SDN Days (GdR CNRS RESCOM) in Loria (Nancy), November 26/27th 2013. Thomas is co-chair (General Chair) of the The 1st International Workshop on Crowdsensing Methods, Techniques, and Applications (CROWDSENSING) organized with IEEE Percom 2014. Thomas is a TPC member of the Named-Oriented Mobility Workshop organized with IEEE Infocom 2014. Thomas was a speaker at the CNRS GdR RESCOM summer school on Information-Centric Networks . Thomas was an invited speaker at the Internet for the Future Society Workshop in Tokyo, organized by the *Societe Franco-Japonaise des Techniques Industrielles* and sponsored by the « Ambassade de France au Japon »

Ye-Qiong Song served as a TPC Member of the following 2013 events: the 18th IEEE international conference on Emerging Technologies & Factory Automation (ETFA'2013) ; the 11th International Conference On Smart homes and health Telematics (ICOST 2013); IROS'13 Workshop on Robots and Sensors integration in future rescue INformation system (ROSIN'13); the International Workshop on Cooperative Robots and Sensor Networks (RoboSense 2013) ; the 12th International Workshop on Real-Time Networks (RTN 2013).

Ye-Qiong Song served as track co-chair of Ubimob2013.

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 par. 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 is the Head of Department of the Charlemagne IUT specialization on multimedia networking.

Olivier Festor is the Director of the TELECOM Nancy Engineering School. Isabelle Chrisment is co-directing the school and is in charge of the students recruitement process. 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.

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 Comitee, 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).

Team members are teaching the following courses:

Abdelkader Lahmadi

- Ecole Ingénieur : Elements of Distributed Computing: algorithms and systems, 20, niveau M2 Ingénieur, ENSEM, France
- Ecole Ingénieur : Wireless Sensor Network Programming, 12, niveau M2 Ingénieur, ENSEM, France
- Ecole Ingénieur : Operating Systems and C language programming, 30, niveau M1 Ingénieur, ENSEM & Ecole des Mines de Nancy, France
- Ecole Ingénieur : Real time systems: concepts and programming, 30, niveau M1 Ingénieur, ENSEM, France
- Ecole Ingénieur : Relational Database, 20, niveau M1 Ingénieur, ENSEM, France
- Ecole Ingénieur : Algorithmic and Programming (Java), 50, niveau L1 Ingénieur, ENSEM, France
- Ecole Ingénieur : Computer Architecture ,50, niveau L1 Ingénieur, ENSEM, France

Bernardetta Addis

- Ecole d'ingénieur : Optimisation Discrete et Deterministe, 21, 2A, Université de Lorraine-ENSMN, France
- Ecole d'ingénieur : Recherche Operationelle, 28, 2A, Université de Lorraine-ENSMN, France

Isabelle Chrisment

- Ecole Ingénieur : Langage C et Shell, 42hTD, niveau L3, Telecom Nancy
- Ecole Ingénieur : Réseaux et Systèmes, 60hTD, niveau M1, Telecom Nancy
- Ecole Ingénieur : Réseaux et Systèmes Avancés, 30hTD, niveau M1, Telecom Nancy
- Ecole Ingénieur : Routage Internet, 50hTD, niveau M2, Telecom Nancy
- Ecole Ingénieur : Sécurité des Réseaux et des Applications, 18hTD, niveau M2, Telecom Nancy

Laurent Andrey

- Licence : Introduction to networks, 56, niveau L1 (DUT), IUT nancy-Charlemagne, France
- Licence : Introduction to network services, 38, niveau L2 (DUT), IUT nancy-Charlemagne, France

Laurent Ciarletta

- Ecole Ingénieur : Networking and Information System, 8, niveau L3 Ingénieur, Mines Nancy, France
- Ecole Ingénieur : Bootcamp (programming bootcamp), 9, niveau M1 Ingénieur, Mines Nancy, France
- Ecole Ingénieur : Operating Systems, 10, niveau M1 Ingénieur, Mines Nancy, France
- Ecole Ingénieur : Networking, 27, niveau M1 Ingénieur, Mines Nancy, France
- Ecole Ingénieur : Advanced Networking and Ambiant Systems, 18, niveau M1 Ingénieur, Mines Nancy, France
- Ecole Ingénieur : Embedded Systems, 18, niveau M1 Ingénieur, Mines Nancy, France
- Ecole Ingénieur : Advanced Software Engineering, 18, niveau M1 Ingénieur, Mines Nancy, France
- Ecole Ingénieur : Android development, 12, niveau M1 and M2 Ingénieur, Collegium Ingenieur and Mines Nancy, France

- Ecole Ingénieur : Ateliers ARTEM "Smart and new workspaces", 90, niveau M1 and M2 Ingénieur, Collegium Ingenieur and Mines Nancy, Nancy National School of Art, ICN Business School, France

Emmanuel Nataf

- DUT : Introduction to computer system and network, 60, niveau L1, IUT nancy-Charlemagne, France
- DUT : Network, 30, niveau L1 , IUT Nancy-Charlemagne, France
- DUT : System, 30, niveau L2, IUT Nancy-Charlemagne, France
- Licence : Network monitoring, 30, niveau L3, IUT Nancy-Charlemagne, France
- Master : Network monitoring, 30, niveau M2, Université de Lorraine, France

Olivier Festor

- Ecole Ingénieur : P2P Algorithms, Protocols and Applications, 12, niveau M2 Ingénieur, Telecom Nancy & ENSEM, France
- Ecole Ingénieur : Voix sur IP, Protocols and Applications, 9, niveau M2 Ingénieur, Telecom Nancy, France

Rémi Badonnel

- Ecole Ingénieur : Networks and Services Management, 24, niveau M2 Ingénieur, TELECOM Nancy, France
- Ecole Ingénieur : Cloud Computing, 22, niveau M2 Ingénieur, TELECOM Nancy, France
- Ecole Ingénieur : Industrial Project, 20, niveau M2 Ingénieur, TELECOM Nancy, France
- Ecole Ingénieur : Networks and Systems, 28, niveau M1 Ingénieur, TELECOM Nancy, France
- Ecole Ingénieur : Advanced Courses on Networks and Systems, 28, niveau M1 Ingénieur, TELECOM Nancy, France
- Ecole Ingénieur : Algorithmics, Data Structures and Algebra, 30, niveau L3 Ingénieur, TELECOM Nancy, France
- Ecole Ingénieur : Design and Development Project, 16, niveau M1 Ingénieur, TELECOM Nancy, France
- Ecole Ingénieur : Initiation to Research Project, 18, niveau M1 Ingénieur, TELECOM Nancy, France
- Ecole Ingénieur : Object-Oriented Programming, 32, niveau L3 Ingénieur, TELECOM Nancy, France
- Ecole Ingénieur : XML Design and Development, 18, niveau L3 Ingénieur, TELECOM Nancy, France

Thibault Cholez

- Ecole Ingénieur : Principles and architecture of computers (ASM), 18h, niveau L3 Ingénieur, TELECOM Nancy, France
- Ecole Ingénieur : C and Shell programming, 22h, niveau L3 Ingénieur, TELECOM Nancy, France
- Ecole Ingénieur : Reliable C++ programming, 10h, niveau M2 Ingénieur, TELECOM Nancy, France

Thomas Silverston

- Master : Réseaux Avancés, 57, niveau M2, Université de Lorraine, France
- Master : Sécurité des réseaux, 45, niveau M2, Université de Lorraine, France
- Master : Architecture des Réseaux, 22, niveau M1, Université de Lorraine

- Master : VoIP, 24, niveau M1, Université de Lorraine
- Master : Introduction aux Réseaux, 26, niveau M2 Math, université de Lorraine, France
- Master : Convergence IP et Mobilité, 24, M2, Université de Lorraine, France
- Ecole d'ingénieur : Voix sur IP, 28, 3A, Telecom Nancy, France
- Master : Convergence et Multimédia, 15, Université de la Réunion

Ye-Qiong Song

- Master : Embedded and Sensor Networks, 8, niveau M2, Université de Lorraine, France
- Ecole Ingénieur : Networking, 40, niveau M2, ENSEM - Université de Lorraine, France
- Ecole Ingénieur : Wireless Sensor Network protocols, 8, niveau M2 Inge´nieur, ENSEM, France
- Ecole Ingénieur : Database, 6, niveau M1, ENSEM - Université de Lorraine, France
- Ecole Ingénieur : Algorithmic and progamming (Java), 90, niveau L3, ENSEM - Université de Lorraine, France
- Ecole Ingénieur : Computer Architecture , 30, niveau L1 Ingénieur, ENSEM, France

9.2.2. Supervision

PhD : Oussema Dabebbi, Dynamic risk management in Voice over IP services, defended the 3rd June 2013, supervised by Remi Badonnel and Olivier Festor

PhD : Juan Pablo Timpanaro, Monitoring and Security in P2P file sharing networks, defended the 6th November 2013, supervised by Isabelle Chrisment

PhD in progress : Martin Barrere, Vulnerability management in autonomic networks and services, since Mar 2011, supervised by Remi Badonnel and Olivier Festor

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 : François Despaux, Delay evaluation in wireless sensor networks for providing QoS, since Oct 2011, supervised by Ye-Qiong Song and Abdelkader Lahmadi

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

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 : Anthéa Mayzaud, Monitoring and Security in the Internet of Things, since May 2013, supervised by Isabelle Chrisment and Remi Badonnel

PhD in progress: Evangelia Tsiontsiou, Multi-constrained QoS routing for wireless sensor networks with applications to smart space for ambient assisted living, since Oct 2013, supervised by Ye-Qiong Song and Bernardetta Addis

PhD in progress : Elian Aubry, Security and Management of Content-Centric Networks, since Oct 2013, supervised by Isabelle Chrisment and Thomas Silverston

PhD in progress : Wazen Shbair, An open and flexible architecture for monitoring the uses of Internet, since Dec. 2013, supervised by Isabelle Chrisment and Thibault Cholez

PhD in progress : Dorin Maxim, Probabilistic Analysis of Real-Time Systems, since Dec 2013, supervised by Françoise Simonot-Lion and Liliana Cucu-Grosjean

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

9.2.3. Juries

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

- Yosra Ben Saied, Ph.D in Computer Science from TELECOM SudParis and Université Pierre et Marie Curie. Title: *Sécurité Collaborative pour l'Internet des Objets*, June 2013. (Isabelle Chrisment)
- Chrystel Gaber, Ph.D. in computer Science from Université de Caen Basse-Normandie. Title: *Sécurisation d'un système de transactions sur terminaux mobiles*. October 2013. (Isabelle Chrisment)
- Leila Benacer, Ph.D in Computer Science from University Paris Est Créteil. Title: *Contributions á l'autodiagnostic de pannes dans les réseaux de communication á large échelle*. December 2013. (Olivier Festor)
- Véronique Legrand , Ph.D in Computer Science from INSA Lyon. Title: *Confiance et risuqe pour engager un échange en milieu hostile*. March 2013. (Olivier Festor)
- Florian Many, Combinaison des aspects temps réel et Sureté de fonctionnement pour la conception des plateformes avioniques, February 2013. (Françoise Simonot-Lion)
- Zhe Li, Ph.D. in Computer Science from TELECOM Bretagne. Title *Optimization d'un réseau de distribution de contenus géré par un opérateur*, January 2013. (Olivier Festor)
- Sylvain Cherrier, Ph.D in Computer Science from University Paris Est. Title: *Architecture et protocoles applicatifs pour la chorégraphie de services dans l'Internet des objets*. December 2013. (Olivier Festor)
- Ludovic Jacquin, Ph.D in Computer Science from University of Grenoble. Title: *Compromis Performance Sécurité pour des passerelles très haut débit pour Internet*, December 2013. (Olivier Festor)
- Jamila Ben Slimane, Ph.D in Computer Science from both University of Lorraine and SupCom Tunis. Title: *Allocation conjointe des canaux de fréquence et des créneaux e temps et routage avec QdS dans les réseaux de capteurs dans fil denses et étendus*, March 2013. (Ye-Qiong Song)
- Xiaoting LI, Ph.D in Computer Science from University of Toulouse - INPT. Title: *Worst-case delay analysis of real-time switched Ethernet networks with flow local synchronization*, September 2013. (Ye-Qiong Song)
- Cédric Mauclair, Ph.D in Computer Science from University of Toulouse - ISAE. Title: *Analyse statistique de réseaux embarqués temps réel*, September 2013. (Ye-Qiong Song)
- Juan Lu, Ph.D in Computer Science from University of Toulouse. Title: *Modeling, simulation and implementation of an 802.15.4 based adaptive communication protocol in wireless sensor network: application to monitoring the elderly at home*, February 2013. (Ye-Qiong Song)
- Mohamed-Anis Gallas, Ph.D in Architecture Science from University of Lorraine. Title: *De l'intégration á la solution architecturale: proposition d'une méthode d'assistance á la prise en compte de la lumière naturelle durant les phases amont de conception*, September 2013. (Ye-Qiong Song)
- Soumeya-Leila Hernane, Ph.D in Computer Science from University of Lorraine. Title: *Modèles et algorithmes de partage de données cohérents pour le calcul parallèle distribué á haut débit*, June 2013. (Ye-Qiong Song)

Team members participated to the following Habilitation Degree defense committees :

- Joaquin Garcia-Alfaro, Habilitation Degree in Computer Science from Université Pierre et Marie Curie Paris 6. Title: *Contributions to the Security of EPC/RFID Wireless Technologies*, 2013. (Olivier Festor)
- Martin Quinson, Habilitation Degree in Computer Science from Université de Lorraine. Title: *Méthodologies d'expérimentation pour l'informatique distribuée à large échelle*, March 2013. (Isabelle Chrisment)

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] O. DABBEBI. , *Gestion des Risques dans les Infrastructures VoIP*, Université de Lorraine, April 2013, http://hal.inria.fr/tel-00875141

[2] J. P. TIMPANARO. , *Hybrid and Anonymous File-Sharing Environments: Architecture and Characterisation*, Université de Lorraine, November 2013, http://hal.inria.fr/tel-00915629

Articles in International Peer-Reviewed Journals

[3] M. BARRÈRE, R. BADONNEL, O. FESTOR. *Vulnerability Assessment in Autonomic Networks and Services: A Survey*, in "Communications Surveys and Tutorials, IEEE Communications Society", August 2013 [*DOI :* 10.1109/SURV.2013.082713.00154], http://hal.inria.fr/hal-00875171

[4] O. DABBEBI, R. BADONNEL, O. FESTOR. *An Online Risk Management Strategy for VoIP Enterprise Infrastructures*, in "Journal of Network and Systems Management", August 2013, 26 p. [*DOI :* 10.1007/s10922-013-9282-4], http://hal.inria.fr/hal-00875133

[5] O. DABBEBI, R. BADONNEL, O. FESTOR. *Leveraging Countermeasures as a Service for VoIP Security in the Cloud*, in "ACM International Journal of Network Management", December 2013 [*DOI :* 10.1002/NEM.1853], http://hal.inria.fr/hal-00926233

Invited Conferences

[6] Y.-Q. SONG. *Reseaux de Capteurs Sans Fil : Comment Fournir La Qualite de Service Tout En Economisant l'Energie ?*, in "Ecole d'été temps réel 2013", Toulouse, France, IRIT Toulouse, August 2013, http://hal.inria.fr/hal-00905864

International Conferences with Proceedings

[7] B. ADDIS, G. CARELLO, E. TÀNFANI. *A Robust Optimization Approach for the Operating Room Planning Problem with Uncertain Surgery Duration*, in "International Conference on Health Care Systems Engineering", Milano, Italy, 2014, vol. 61, pp. 175-189 [*DOI :* 10.1007/978-3-319-01848-5_14], http://hal.inria.fr/hal-00914689

[8] M. BARRÈRE, R. BADONNEL, O. FESTOR. *Improving Present Security through the Detection of Past Hidden Vulnerable States*, in "IFIP/IEEE International Symposium on Integrated Network Management (IM'13)", Ghent, Belgium, May 2013, http://hal.inria.fr/hal-00875199

[9] M. BARRÈRE, G. HUREL, R. BADONNEL, O. FESTOR. *A Probabilistic Cost-efficient Approach for Mobile Security Assessment*, in "IFIP/IEEE International Conference on Network and Service Management (CNSM'13)", Zurich, Switzerland, October 2013, http://hal.inria.fr/hal-00875219

[10] M. BARRÈRE, G. HUREL, R. BADONNEL, O. FESTOR. *Ovaldroid: an OVAL-based Vulnerability Assessment Framework for Android*, in "IFIP/IEEE International Symposium on Integrated Network Management (IM'13)", Ghent, Belgium, IEEE, May 2013, http://hal.inria.fr/hal-00875212

[11] C. BERNARDINI, T. SILVERSTON, O. FESTOR. *Cache Management Strategy for CCN based on Content Popularity*, in "AIMS - 7th International Conference on Autonomous Infrastructure, Management and Security", Barcelonne, Spain, G. DOYEN, M. WALDBURGER, P. ČELEDA, A. SPEROTTO, B. STILLER (editors), Lecture Notes in Computer Science, Springer, July 2013, vol. 7946, pp. 92-95 [*DOI :* 10.1007/978-3-642-38998-6_12], http://hal.inria.fr/hal-00929736

[12] C. BERNARDINI, T. SILVERSTON, F. OLIVIER. *MPC: Popularity-based Caching Strategy for Content Centric Networks*, in "Communications (ICC), 2013 IEEE International Conference on", Budapest, Hungary, IEEE, November 2013, pp. 3619 - 3623 [*DOI :* 10.1109/ICC.2013.6655114], http://hal.inria.fr/hal-00929737

[13] L. CIARLETTA, V. CHEVRIER, T. NAVARRETE GUTIERREZ. *Multi-agent simulation based governance of complex systems : architecture and example implementation on free-riding*, in "ENC 2013, Mexican International Conference on Computer Science", MORELIA, Mexico, October 2013, http://hal.inria.fr/hal-00905235

[14] F. DESPAUX, Y.-Q. SONG, A. LAHMADI. *Measurement-based Analysis of the Effect of Duty Cycle in IEEE 802.15.4 MAC Performance*, in "CSCPS - 1st International Workshop on Compressive Sensing in Cyber-Physical Systems - 2013", Hangzhou, China, October 2013, http://hal.inria.fr/hal-00877466

[15] F. DESPAUX, Y.-Q. SONG, A. LAHMADI. *On the Gap Between Mathematical Modeling and Measurement Analysis for Performance Evaluation of the 802.15.4 MAC Protocol*, in "RTN - 12th International Workshop on Real-Time Networks - 2013", Paris, France, July 2013, http://hal.inria.fr/hal-00877452

[16] A. LAHMADI, A. BOEGLIN, O. FESTOR. *Efficient Distributed Monitoring in 6LoWPAN Networks*, in "CNSM - 9th International Conference on Network and Service Management - 2013", Zurich, Switzerland, University of Zürich, October 2013, http://hal.inria.fr/hal-00879550

[17] A. MAYZAUD, R. BADONNEL, I. CHRISMENT. *Monitoring and Security for the Internet of Things*, in "AIMS - 7th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security", Barcelona, Spain, G. DOYEN, M. WALDBURGER, P. ČELEDA, A. SPEROTTO, B. STILLER (editors), Springer, June 2013, pp. 37-40 [*DOI :* 10.1007/978-3-642-38998-6_4], http://hal.inria.fr/hal-00876216

[18] E. NATAF, O. FESTOR. *Accurate Online Estimation of Battery Lifetime for Wireless Sensors Network*, in "SENSORNETS - 2nd International conference on sensor networks", Barcelone, Spain, M. VAN SINDEREN, O. POSTOLACHE, C. BENAVENTE-PECES (editors), SCITEPRESS, 2013, http://hal.inria.fr/hal-00875536

[19] M. S. SEDDIKI, N. BILEL, Y.-Q. SONG, M. FRIKHA. *Queuing analysis of dynamic resource allocation for virtual routers*, in "ISCC - The 18th IEEE symposium on Computers and Communications - 2013", Split, Croatia, July 2013, http://hal.inria.fr/hal-00877581

[20] M. S. SEDDIKI, B. NEFZI, Y.-Q. SONG, M. FRIKHA. *Automated Controllers for Bandwidth Allocation in Network Virtualization*, in "IPCCC - 32nd IEEE International Performance Computing and Communications Conference - 2013", San Diego, United States, December 2013, http://hal.inria.fr/hal-00877579

[21] M. S. SEDDIKI, Y.-Q. SONG, M. FRIKHA. *Dynamic node allocation in Network Virtualization*, in "HPCS - The 2013 International Conference on High Performance Computing & Simulation - 2013", Helsinki, Finland, July 2013, http://hal.inria.fr/hal-00877580

[22] J. P. TIMPANARO, I. CHRISMENT, O. FESTOR. *Monitoring Anonymous P2P File-Sharing Systems*, in "IEEE P2P 2013 - Poster Session", Trento, Italy, September 2013, 2 p. , http://hal.inria.fr/hal-00915618

[23] S. ZHUO, Z. WANG, Y.-Q. SONG, Z. WANG, A. LUIS. *iQueue-MAC: A Traffic Adaptive duty-cycled MAC Protocol With Dynamic Slot Allocation*, in "IEEE SECON", New Orleans, United States, IEEE, June 2013, pp. 95-103 [*DOI :* 10.1109/SAHCN.2013.6644967], http://hal.inria.fr/hal-00905822

National Conferences with Proceedings

[24] M. CHEHAIDER, K. ROUSSEL, Y.-Q. SONG. *Interopérabilité des réseaux de capteurs hétérogènes dans un appartement intelligent*, in "UbiMob - 9èmes journées francophones Mobilité et Ubiquité - 2013", Nancy, France, June 2013, http://hal.inria.fr/hal-00877451

[25] E. FINICKEL, A. LAHMADI, O. FESTOR. *Vers une detection automatique des applications malveillantes dans les environnements Android*, in "UbiMob - 9èmes journées francophones Mobilité et Ubiquité - 2013", Nancy, France, June 2013, http://hal.inria.fr/hal-00879614

Scientific Books (or Scientific Book chapters)

[26] N. NAVET, F. SIMONOT-LION. *In-vehicle communication networks - a historical perspective and review*, in "Industrial Communication Technology Handbook, Second Edition", R. ZURAWSKI (editor), CRC Press Taylor&Francis, 2013, http://hal.inria.fr/hal-00876524

Research Reports

[27] M. BARRÈRE, R. BADONNEL, O. FESTOR. , *A SAT-based Autonomous Strategy for Security Vulnerability Management*, September 2013, 8 p. , http://hal.inria.fr/hal-00875240

[28] C. BERNARDINI, T. SILVERSTON, O. FESTOR. , *Using Social Network Information into ICN*, April 2013, It was presented at NOMEN 2013 as a poster. NOMEN 2013 was a workshop held in IEEE INFOCOM 2013, http://hal.inria.fr/hal-00819089

[29] L. CIARLETTA, V. GALTIER, A. GUENARD, Y. PRESSE. , *Using a flock of UAVs as a CPS and platform for application-driven research*, June 2013, http://hal.inria.fr/hal-00912714

[30] P. O. KAMGUEU, E. NATAF, T. DJOTIO NDIÉ, O. FESTOR. , *Energy-based routing metric for RPL*, Inria, January 2013, n^{o} RR-8208, 14 p. , http://hal.inria.fr/hal-00779519

[31] B. LAMAS, A. SOURY, B. SAADALLAH, A. LAHMADI, O. FESTOR. , *An Experimental Testbed and Methodology for Security Analysis of SCADA Systems*, Inria, December 2013, n^{o} RT-0443, 89 p. , http://hal.inria.fr/hal-00920828

Other Publications

[32] Y. ABID. , *In-network processing in Wireless Sensor Networks using a content centric approach*, September 2013, http://hal.inria.fr/hal-00922101

[33] B. ADDIS, G. CARELLO, A. CAPONE, L. GIANOLI, B. SANSÒ. , *Robust Energy Management for Green and Survivable IP Networks*, 2013, http://hal.inria.fr/hal-00926122

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

[35] B. ADDIS, G. CARELLO, E. TÀNFANI. , *A robust optimization approach for the Advanced Scheduling Problem with uncertain surgery duration in Operating Room Planning*, 2014, http://hal.inria.fr/hal-00936019

[36] L. ANDREY, O. FESTOR. , *VAMPIRE - Analyse, observation et prévention de vulnérabilités dans l'Internet du futur - Compte-rendu de fin de projet*, February 2013, Rapport final du projetProjet ANR-08-VERS-017 (Vampire), http://hal.inria.fr/hal-00913723

[37] S. ANNA, A. MAYZAUD. , *Initial Deliverable on Network and Service Monitoring (Deliverable 5.1, Flamingo NoE)*, October 2013, Project Deliverable, http://hal.inria.fr/hal-00926187

[38] T. CHOLEZ. *Management of Content-Centric Networking*, in "ResCom 2013: Les réseaux centrés sur les contenus, Évolution ou révolution de l'Internet ?", Porquerolles, France, May 2013, ResCom 2013: Les réseaux centrés sur les contenus, Évolution ou révolution de l'Internet ?, http://hal.inria.fr/hal-00924363

[39] N. DEROUICHE. , *Monitoring of the Anonymous I2P Network*, November 2013, http://hal.inria.fr/hal-00926586

[40] O. FESTOR, R. BADONNEL. , *First Year Report on Standardization (Deliverable D4.1, Flamingo NoE)*, October 2013, Project Deliverable, http://hal.inria.fr/hal-00926172

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

[42] R. GABI DREO, A. MAYZAUD, A. LAHMADI, R. BADONNEL, H. GAETAN. , *First Year Report on Automated Configuration and Repair (Deliverable D6.1, Flamingo NoE)*, October 2013, Project Deliverable, http://hal.inria.fr/hal-00926198

[43] G. HUREL. , *Detection externalisée de vulnerabilités pour la plateforme Android à l'aide du langage OVAL*, LORIA - Université de Strasbourg, June 2013, http://hal.inria.fr/hal-00875179

[44] G. MARKUS, B. MARTIN, R. BADONNEL, O. FESTOR. , *Handbook on Optimization, Learning, Operation and Cooperation Methods (Deliverable D3.9, Univerself Project)*, August 2013, Project Deliverable, http://hal.inria.fr/hal-00925505

[45] D. PANAGIOTIS, B. MARTIN, R. BADONNEL, O. FESTOR. , *Synthesis of Deployment Results (Deliverable D4.12, Univerself Project)*, November 2013, Project Deliverable, http://hal.inria.fr/hal-00925485

[46] F. REBHI. , *Development of a tool for analysis and visualization of Android logs*, Ecole Nationale des Sciences de l'Informatique (ENSI) - Tunisie, September 2013, http://hal.inria.fr/hal-00922034

[47] A. SOURY. , *Génération automatique de règles de sécurité pour les réseaux SCADA*, July 2013, http://hal.inria.fr/hal-00922058

[48] J. VAUBOURG. , *Export de NetFlows 9 sous Android et Inférence de la localisation d'un utilisateur d'ordiphone sans données géotagguées*, September 2013, http://hal.inria.fr/hal-00922061

References in notes

[49] 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