Activity Report 2017

Team MADYNES

Management of dynamic networks and services

Inria teams are typically groups of researchers working on the definition of a common project, and objectives, with the goal to arrive at the creation of a project-team. Such project-teams may include other partners (universities or research institutions).

RESEARCH CENTER
Nancy - Grand Est

THEME
Networks and Telecommunications

Table of contents

Team MADYNES

Creation of the Project-Team: 2004 February 01, updated into Team: 2017 January 19, end of the Team: 2017 December 31

Keywords:

Computer Science and Digital Science:

A1.1.4. - High performance computing
A1.1.6. - Cloud
A1.1.7. - Peer to peer
A1.1.8. - Security of architectures
A1.2. - Networks
A1.3. - Distributed Systems
A1.5. - Complex systems
A2.6. - Infrastructure software
A3.1.1. - Modeling, representation
A3.1.3. - Distributed data
A3.2.2. - Knowledge extraction, cleaning
A3.2.3. - Inference
A3.3. - Data and knowledge analysis
A3.4. - Machine learning and statistics
A4.1. - Threat analysis
A4.4. - Security of equipment and software
A4.9. - Security supervision
A6.1.2. - Stochastic Modeling (SPDE, SDE)
A6.1.3. - Discrete Modeling (multi-agent, people centered)
A6.1.5. - Multiphysics modeling
A6.2.6. - Optimization

Other Research Topics and Application Domains:

B2.5.3. - Assistance for elderly
B4.5. - Energy consumption
B5.1. - Factory of the future
B6.3.2. - Network protocols
B6.3.3. - Network Management
B6.4. - Internet of things
B6.5. - Information systems
B6.6. - Embedded systems
B8.1. - Smart building/home
B8.5. - Smart society
B9.5.10. - Digital humanities
B9.6. - Reproducibility

1. Personnel

Research Scientists

Raouf Boutaba [Inria, International Chair, Advanced Research Position]
Olivier Festor [Univ de Lorraine, Senior Researcher, HDR]
Jérôme François [Inria, Researcher]
Dorin Maxim [Univ de Lorraine, Researcher]
Vassili Rivron [Inria, Researcher, until Aug 2017]

Faculty Members

Isabelle Chrisment [Team leader, Univ de Lorraine, Professor, HDR]
Laurent Andrey [Univ de Lorraine, Associate Professor]
Rémi Badonnel [Univ de Lorraine, Associate Professor]
Thibault Cholez [Univ de Lorraine, Associate Professor]
Laurent Ciarletta [Univ de Lorraine, Associate Professor]
Abdelkader Lahmadi [Univ de Lorraine, Associate Professor]
Emmanuel Nataf [Univ de Lorraine, Associate Professor]
Lucas Nussbaum [Univ de Lorraine, Associate Professor]
Ye-Qiong Song [Univ de Lorraine, Professor, HDR]

Post-Doctoral Fellows

Benoit Henry [Univ de Lorraine, until Sep 2017]
Zhixiang Liu [Univ de Lorraine, until Aug 2017]

PhD Students

Elian Aubry [Univ de Lorraine, until Oct 2017]
Pierre-Olivier Brissaud [Thales]
Paul Chaignon [Orange Labs]
Maxime Compastié [Orange Labs]
Virgile Dauge [Univ de Lorraine, from Apr 2017]
Giulia de Santis [Inria]
Florian Greff [Thales & Univ. Lorraine, granted by CIFRE]
Patrick Kamgueu [Univ. Lorraine, granted by Ministry of Foreign Affairs, since Jun 2012, in co-supervision with Université de Yaounde]
Daishi Kondo [CNRS]
Mingxiao Ma [Univ de Lorraine, from Sep 2017 until Nov 2017]
Xavier Marchal [CNRS]
Thomas Paris [Univ de Lorraine]
Abdulqawi Saif [Xilopix, granted by CIFRE]
Nicolas Schnepf [Inria]
Salvatore Signorello [University of Luxembourg - Univ. Lorraine (co-advising)]
Evangelia Tsiontsiou [Univ de Lorraine, until Oct 2017]
Julien Vaubourg [Univ de Lorraine, until Aug 2017]
Louis Viard [Univ de Lorraine, from Nov 2017]
Haftay Gebreslasie Abreha [Cynapsys, granted by CIFRE]

Technical staff

Soline Blanc [Inria, from Sep 2017]
François Despaux [Univ de Lorraine]
Florent Didier [Inria]
Thomas Lacour [Inria, from Sep 2017]
Sofiane Lagraa [Inria, until Sep 2017]
Alexandre Merlin [Inria, from Mar 2017]
Yannick Presse [Inria, until Mar 2017, granted by EDF]

Loic Rouch [Inria]
Wazen Shbaïr [CNRS, until Apr 2017]
Alexandre Tan [Inria, until Mar 2017]
Shuguo Zhuo [Inria]
Arthur Garnier [Inria, until Aug 2017]

Interns

Petro Aksonenko [Univ de Lorraine]
Paul Arduin [Inria, from Jun 2017 until Aug 2017]
Souha Bel Haj Hassine [Univ de Lorraine, from Apr 2017 until Oct 2017]
Norhane Benkahla [Univ de Lorraine, from Oct 2017]
Yutian Chen [Inria, from Jun 2017 until Aug 2017]
Romain Deniaux [Univ de Lorraine, from Jun 2017 until Aug 2017]
Grégoire Domerc [Inria, from Jul 2017 until Sep 2017]
Laurent Evrard [Inria, from Sep 2017]
Arouna Ganou [Inria, from Jul 2017 until Sep 2017]
Mahdi Gharbi [Inria, from Jul 2017 until Aug 2017]
Lucas Gourmelon [Inria, from Apr 2017 until Jun 2017]
Abdellah Houmz [Internship UIR, from Nov 2017]
Maxime Josse [Univ de Lorraine, from Mar 2017 until Aug 2017]
John Mains [Univ de Lorraine, from May 2017 until Jun 2017]
Daniel Martin [Univ de Lorraine, until Feb 2017]
Arthur Perret [Inria, from Apr 2017 until Jul 2017]
Andrew Singletary [Univ de Lorraine, from May 2017 until Jul 2017]
Teddy Valette [Inria, from Apr 2017 until Jul 2017]
Mehdi Zakroum [Internship UIR, from Nov 2017]

Administrative Assistants

Isabelle Herlich [Inria]
Delphine Hubert [Univ de Lorraine]
Annick Jacquot [Inria]
Martine Kuhlmann [CNRS]
Sylvie Musilli [Univ de Lorraine]
Bertrand Wallrich [Inria]

Visiting Scientists

Juan Pablo Afman [Univ de Lorraine, from May 2017 until Jul 2017]
Thomas Gurriet [from May 2017 until Jul 2017]

2. Overall Objectives

2.1. Overall Objectives

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

The project develops applied research activities in the following areas:

- **Autonomous Management**:
  - the design of models and methods enabling *self-organization and self-management* of networked entities and services,
  - the evaluation of management architectures based on *peer-to-peer and overlay principles*,
  - the investigation of novel approaches to the representation of *management information*,
  - the modeling and *performance evaluation* of dynamic networks.
- **Functional Areas** instantiate autonomous management functions:
  - the *security plane* where we focus on building closed-loop approaches to protect networking assets,
  - the *service configuration* where we aim at providing solutions covering the delivery chain from device discovery to QOS-aware delivery in dynamic networks,
  - *monitoring* where we aim at building solutions to characterize and detect unwanted service behavior.

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

3. Research Program

3.1. Evolutionary needs in network and service management

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

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

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

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

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

4. Application Domains

4.1. Mobile 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 mainly focus at the network level on mobile devices and Internet of Things. We are investigating the provisioning, monitoring, configuration and performance management issues.

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,
- cyber-physical systems,
- information centric networks,
- distributed cloud environnements,
- smart environments.

5. Highlights of the Year

5.1. Highlights of the Year

- The team (Jérôme François and Lucas Nussbaum) organized the Cloud Days (GdR CNRS RSD, Virtualizaion and Cloud Action) in Loria (Nancy).
- Loic Rouch demonstrated in Blackhat Europe 2017 an attack to tack over a z-wave network https://www.blackhat.com/eu-17/briefings/schedule/#a-universal-controller-to-take-over-a-z-wave-network-8459.

BEST PAPER AWARD:

[17]
S. LAGRAA, J. FRANCOIS. *Knowledge Discovery of Port Scans from Darknet*, in "IFIP/IEEE Symposium on Integrated Network and Service Management (IM) - AnNet workshop", Lisbonne, Portugal, May 2017, https://hal.archives-ouvertes.fr/hal-01636215

6. New Software and Platforms

6.1. Distem

KEYWORDS: Large scale - Experimentation - Virtualization - Emulation
FUNCTIONAL DESCRIPTION: Distem is a distributed systems emulator. When doing research on Cloud, P2P, High Performance Computing or Grid systems, it can be used to transform an homogenenous cluster (composed of identical nodes) into an experimental platform where nodes have different performance, and are linked together through a complex network topology, making it the ideal tool to benchmark applications targetting such environments, or aiming at tolerating performance degradations or variations which are frequent in the Cloud or in other applications distributed at large scale (P2P for example).

- Participants: Luc Sarzyniec, Lucas Nussbaum and Tomasz Buchert
- Partners: CNRS - Université de Lorraine - Loria - Grid'5000 - Inria
- Contact: Lucas Nussbaum
- URL: http://distem.gforge.inria.fr

6.2. Grid’5000 testbed

FUNCTIONAL DESCRIPTION: Grid’5000 is a scientific instrument designed to support experiment-driven research in all areas of computer science related to parallel, large-scale or distributed computing and networking. It gathers 10 sites, 25 clusters, 1200 nodes, for a total of 8000 cores. It provides its users with a fully reconfigurable environment (bare metal OS deployment with Kadeploy, network isolation with KaVLAN) and a strong focus on enabling high-quality, reproducible experiments.

- Participants: Arthur Garnier, Clement Parisot, Émile Morel, Emmanuel Jeanvoine, Jérémie Gaidamour, Luc Sarzyniec and Lucas Nussbaum
- Contact: Lucas Nussbaum
- URL: https://www.grid5000.fr/

6.3. Kadeploy

KEYWORD: Operating system provisioning
FUNCTIONAL DESCRIPTION: Kadeploy is a scalable, efficient and reliable deployment (provisioning) system for clusters and grids. It provides a set of tools for cloning, configuring (post installation) and managing cluster nodes. It can deploy a 300-nodes cluster in a few minutes, without intervention from the system administrator. It plays a key role on the Grid’5000 testbed, where it allows users to reconfigure the software environment on the nodes, and is also used on a dozen of production clusters both inside and outside Inria.

- Participants: Emmanuel Jeanvoine, Luc Sarzyniec and Lucas Nussbaum
- Partners: CNRS - Université de Lorraine - Loria - Grid’5000 - Inria
- Contact: Lucas Nussbaum
- URL: http://kadeploy3.gforge.inria.fr

6.4. MECSYCO-RE-C++

en Multi-agent Environment for Complex SYstems COsimulation. Coeur C++
KEYWORDS: Agent - Multi-agent - Multi-model - Simulator - Simulation - Modeling - Artefact
FUNCTIONAL DESCRIPTION: MECSYCO is a project aiming at the modeling and simulation of complex systems. It provides concepts and tools to describe and then simulate a system as a set of heterogeneous models (namely a multi-model). MECSYCO-RE-C++ is the C++ implementation of the central part (core) of MECSYCO. It can be complimente by mecsyco-com (a communication package for distributed exécution) and mecsyco-visu (a set of tools for vizualizaing simulations).

- Participants: Benjamin Camus, Benjamin Segault, Julien Vaubourg, Laurent Ciarletta, Nicolas Kirchner, Victorien Elvinger, Vincent Chevrier and Yannick Presse
- Partners: Université de Lorraine - Inria
- Contact: Vincent Chevrier

6.5. MECSYCO-RE-java

Multi-agent Environment for Complex SYstems COsimulation. Coeur java
KEYWORDS: Agent - Multi-agent - Co-simulation - Multi-model - Simulator - Simulation - Modeling - Artefact

FUNCTIONAL DESCRIPTION: MECSYCO is a project aiming at the modeling and simulation of complex systems. It provides concepts and tools to describe and then simulate a system as a set of heterogeneous models (namely a multi-model). MECSYCO-RE-java is the Java implementation of the central part (core) of MECSYCO. It can be complemented by mecsyco-com (a communication package for distributed exécution) and mecsyco-visu (a set of tools for vizualizaing simulations).

- Participants: Benjamin Camus, Christine Bourjot, Julien Siebert, Julien Vaubourg, Laurent Ciarletta, Victorien Elvinger, Vincent Chevrier and Yannick Presse
- Partners: Université de Lorraine - Inria
- Contact: Vincent Chevrier
- URL: http://www.mecsyco.com

6.6. Ruby-cute

KEYWORDS: Experimentation - HPC - Cloud
FUNCTIONAL DESCRIPTION: Ruby-Cute is a set of Commonly Used Tools for Experiments, or Critically Useful Tools for Experiments, depending on who you ask. It is a library aggregating various Ruby snippets useful in the context of (but not limited to) development of experiment software on distributed systems testbeds such as Grid'5000.

- Contact: Lucas Nussbaum
- URL: http://ruby-cute.github.io/

6.7. Platforms

6.7.1. CPS Security Assessment Platform

This year, we have extended our Cyber-Physical systems security assessment platform with new hardware components including multiple types of Programmable Logic Controllers (PLS) and a small scale distribution and sorting testbed. The physical platform is also extended with several IoT devices dedicated to residential networks (heating control, lightning system, home gateways, etc). The platform will be mainly used for building security assessmenet and evaluation experimentation on the available devices to identify and validate their associated attack patterns and discover new vulnerabilities.

7. New Results

7.1. Monitoring

7.1.1. Quality of Experience Monitoring

Participants: Isabelle Chrisment [contact], Thibault Cholez, Vassili Rivron, Lakhdar Meftah [University of Lille].

We have pursued our work on smartphone usage monitoring with the SPIRALS team (Inria/Université de Lille) and more specifically on proposing new methods to help measure the QoE and to protect the user's privacy when collecting such data.

In parallel, to evaluate our methods, we need a testing framework to automate testing of WiFi P2P mobile apps at scale. In [20] we proposed AndroFleet, a large-scale WiFi P2P testing framework. Androfleet can perform User Acceptance Testing for a fleet of emulators, by emulating the hardware behavior of the peer discovery, it gives the developers the ability to control P2P specific behaviors (peers joining and leaving).

7.1.2. Active Monitoring

Participants: Abdelkader Lahmadi [contact], Jérôme François, Frédéric Beck [LHS], Loic Rouch [LHS].

Following the work done in 2016, we pursued our collaboration with the regional PME TracIP (http://www.tracip.fr) on the development of attack assessment and forensics platform dedicated to industrial control systems. The platform involves multiple PLC from different manufacturers and real devices of factory automation systems (see 6.7.1).

During the year 2017, we have demonstrated that off-the-shelf hardware is sufficient to take over any Z-Wave network without knowing its topology or compromising any original devices and remaining unnoticeable for the primary controller. Our attack consists in building an adversary Z-Wave universal controller by reprogramming a mainstream USB stick controller. The technique exploits two features provided by the USB stick which allow (1) to set the network identifier (HomeID) and (2) to learn many devices identifiers even if they are not physically available. The attack has been demonstrated in Blackhat Europe 2017 by Loic Rouch (https://www.blackhat.com/eu-17/briefings/schedule/#a-universal-controller-to-take-over-a-z-wave-network-8459).

7.1.3. Service-level Monitoring of HTTPS traffic

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

We previously proposed an alternative technique to investigate HTTPS traffic which aims to be robust, privacy-preserving and practical with a service-level identification of HTTPS connections, i.e. to name the services, without relying on specific header fields that can be easily altered. We have defined dedicated features for HTTPS traffic that are used as input for a multi-level identification framework based on machine learning algorithms processing full TLS sessions. Our evaluation based on real traffic shows that we can identify encrypted web services with a high accuracy. In 2017, we finished to develop our solution to make it fully usable in real-time [1]. We now provide our prototype implementation (https://gitlab.inria.fr/swazen/HTTPSFirewall) in open-source. It operates by extending the iptables/netfilter architecture. It receives and demultiplexes the arriving HTTPS packets to a related flow. As soon as the number of packets in a given flow reaches a threshold, the identification engine extracts the features and runs the C4.5 algorithm to predict the HTTPS service of the flow.

7.1.4. Monitoring Programmable Networks

Participants: Jérôme François [contact], Olivier Festor, Paul Chaignon [Orange Labs], Kahina Lazri [Orange Labs], Thibault Delmas [Orange Labs].

Software-Defined Networking brings new capabilities in operating networks including monitoring. In the state-of-the art many proposals have been made to enhance monitoring of networks using OpenFlow or other proposed programmable frameworks. In a preliminary work [11], we reviewed them in order to highlight what are the remaining challenges to be addressed in that area. The main issue is the trade-off to be made between the strong expressibility (especially stateful operations) and capability of monitoring techniques that are necessary for advanced operation purposes and the complexity it induces if we want to keep the pace with line-rate packet processing. Another important aspect is the security as adding programmable monitoring functions may lead to introduce security threats. Our current work is thus focused on adding monitoring capacity while guaranteeing line-rate operations and safety requirements even when programs are deployed on running network switches.

7.1.5. Smart Contracts Monitoring

Participants: Jérôme François [contact], Sofiane Lagraa, Radu State [University of Luxembourg], Jérémy Charlier [University of Luxembourg].

Blockchain technologies are skyrocketing and the team is interested in assessing the impact of such technologies on networking, and if necessary managing the coupling between them. Indeed, blockchain efficiency resides in an overlay network built on top of a real infrastructure which needs to properly support it. Orchestrating network ressources, *i.e.* adding some network capacity, might be helpful but supposes first an in-depth monitoring of blockchain interactions. In a first work, we thus evaluated the relation among smart contracts. We defined methods to discover smart contracts interactions and the different group properties. This approach relies on graph modelling and mining techniques as well as tensor modelling combined with stochastic processes. It underlines actual exchanges between smart contracts and targets the predictions of future interactions among the communities. Comparative study between graph analysis and tensor analysis is provided for predictions of smart contract interactions. Finally, virtual reality visualization based on Unity 3D game engine has been applied [12].

7.1.6. Sensor networks monitoring

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

Our work on IoT security monitoring has been published in IEEE Transactions on Network and Service Management [4]. This concerns more specifically our distributed monitoring architecture for detecting attacks against RPL networks. The RPL routing protocol has been standardized by IETF to enable a lightweight and robust routing in lower-power and lossy networks. After having compared existing IoT monitoring solutions, we have proposed a detection strategy for RPL version number attacks. This one relies on our monitoring architecture to preserve constrained node resources, in the context of AMI infrastructures. A versioning mechanism is incorporated into RPL in order to maintain an optimized topology. However, an attacker can exploit this mechanism to significantly damage the network and reduce its lifetime. We have exploited monitoring node collaboration to identify the attacker, the localization process being performed by the root after gathering detection information from all monitoring nodes. We have evaluated our solution through experiments and have analyzed the performance according to defined metrics. We have shown that the false positive rate of our solution can be reduced by a strategic monitoring node placement. We have also considered the scalability issue, by modeling this placement as an optimization problem and quantifying the number of required monitoring nodes to ensure acceptable false positive rates.

7.2. Security

7.2.1. Security analytics

Participants: Jérôme François [contact], Abdelkader Lahmadi, Sofiane Lagraa, Soline Blanc, Giulia de Santis, Olivier Festor, Radu State [University of Luxembourg], Christian Hammerschmidt [University of Luxembourg].

In 2017, we have continued our active cooperation with the High Security Lab (HSL) in Nancy. The latter provides the infrastructure to support two main projects in security analytics, namely the FUI HuMa project and the ATT AMICS. Thanks to darknet data of the HSL, we developped two methods based on graph-mining to extract knowledge. The first one focuses on port scanning analysis in order to profile the behaviours and patterns of attackers. By representing consecutive targeted ports in an aggregated graph format, we assess then the centrality of port number using different metrics and highlights valuable correlation among some of them. We are particularly able to identify patterns of scanning related to a specific setup (e.g. medical environment) [17]. We then extended this method to security events analysis by constructing multiple graphs to be analyzed with an outlier technique. The rationale is to represent individual behaviors and detect those which deviate from the majority. The method has been successfully applied to botnet detection in [16]. We are currently leveraging our graph analysis in order to provide to the community a new metric or distance to be applied when comparing port numbers. Indeed, numerical comparison is meaningless in that context and we could leverage either a semantic database (such as Wikipedia) or attacker database (darknet) to derive a meaningful metric, *i.e.* representing a real correlation between port numbers (TCP or UDP).

Furthermore, we continue our work on using Hidden Markov Models for analysing TCP scanning activities. We are now in a stage where individual models from different scanner tools or configurations (e.g. targeted ports) are used in order to automatically learn unique signatures then applied on non-labelled data.

7.2.2. NDN Security

Participants: Thibault Cholez [contact], Xavier Marchal, Olivier Festor, Jérôme François, Salvatore Signorello [University of Luxembourg], Radu State [University of Luxembourg], Samuel Marchal [Aalto University].

Information Centric Networking (ICN) is seen as a promising solution to re-conciliate the Internet usage with its core architecture. However, to be considered as a realistic alternative to IP, ICN must evolve from a pure academic proposition deployed in test environments to an operational solution in which security is assessed from the protocol design to its running implementation. Among ICN solutions, Named Data Networking (NDN), together with its reference implementation NDN Forwarding Daemon (NFD), acts as the most mature proposal but its vulnerability against the Content Poisoning Attack (CPA) is considered as a critical threat that can jeopardize this architecture. So far, existing works in that area have fallen into the pit of coupling a biased and partial phenomenon analysis with a proposed solution, hence lacking a comprehensive understanding of the attack's feasibility and impact in a real network. In a joint work with our colleagues from UTT and in the context of the ANR DOCTOR projet, we demonstrated through an experimental measurement campaign that CPA can easily and widely affect NDN. Our contribution is threefold: (1) we propose three realistic attack scenarios relying on both protocol design and implementation weaknesses; (2) we present their implementation and evaluation in a testbed based on the latest NFD version; and (3) we analyze their impact on the different ICN nodes (clients, access and core routers, content provider) composing a realistic topology. This work was published in IM 2017 conference [21].

Also, still in the context of the DOCTOR project, we refined our architecture to securely deploy NDN over NFV. Indeed, combining NFV fast service deployment and SDN fine grained control of data flows allows comprehensive network security monitoring. The DOCTOR architecture allows detecting, assessing and remediating attacks. NDN is an example of application made possible by SDN and NFV coexistence, since hardware implementation would be too expensive. We showed how NDN routers can be implemented and managed as VNFs. Security monitoring of the DOCTOR architecture is performed at two levels. First, host-level monitoring, provided by CyberCAPTOR, uses an attack graph approach based on network topology knowledge. It then suggests remediations to cut attack paths. We show how our monitoring tool integrates SDN and NFV specificities and how SDN and NFV make security monitoring more efficient. Then, application-level monitoring relies on the MMT probe. It monitors NDN-specific metrics from inside the VNFs and a central component can detect attack patterns corresponding to known flaws of the NDN protocol. These attacks are fed to the CyberCAPTOR module to integrate NDN attacks in attack graphs. This work was published in a book chapter "Guide to Security in SDN and NFV" from Springer's Computer Communications and Networks collection [35].

Finally, in cooperation with the University of Luxembourg, we have investigated interest flooding attacks in NDN. By nature, NDN communication assumes that requesting a content leads to emit an interest and forwarding it in the network until it reaches an appropriate content provider which then sends back data through the reverse path. Interest flooding attacks forge interests (requests) which cannot be satisfied by any data to be sent back to the emitter. As such, both the network and nodes are overloaded as the interests are flooded into the network and intermediate nodes have to store them locally in the pending interest table. We observed that most of literature mechanisms have been evaluated with very simple attack models. Actually, we had a great expertise in phishing attacks and social engineering that can be used to generate realistic phishing names for the NDN naming scheme. We thus create a new stealthy attack relying on natural language processing techniques to forge interests very similar to legitimate ones making inefficient all proposed counter-measures from the state-of-the-art [25].

7.2.3. Configuration security automation

Participants: Rémi Badonnel [contact], Abdelkader Lahmadi, Olivier Festor, Nicolas Schnepf, Maxime Compastié.

The main research challenge addressed in this work is focused on enabling configuration security automation in dynamic networks and services. In particular our objective is to support the efficient configuration and orchestration of security management operations.

The continuous growth and variety of networking significantly increases the complexity of management. It requires novel autonomic methods and techniques contributing to detection and prevention performances with respect to vulnerabilities and attacks.

We have pursued during Year 2017 the efforts on the orchestration of security functions in the context of mobile smart environments, with our joint work with Stephan Merz of the VeriDis project-team at Inria Nancy. We had already defined an automated verification technique, based on an extension of an SDN language, for checking both the control and the data planes related to security chains [24]. Complementarily, we proposed a strategy for generating SDN policies for protecting Android environments based on automata learning. Our solution collects traces of flow interactions of their applications, aggregates them in order to build finite-state models, and then infer SDN policy rules. We have designed and implemented aggregation and automata learning algorithms that allow precise and generic models of applications to be built. These models will be then used for configuring chains of security functions specified in the Pyretic language and verified with our Synaptic checker. We have developed a prototype of our solution implementing these algorithms, and evaluated its performances through a series of experiments based on the backend process miners Synoptic and Invarimint, in addition to our own algorithm. The experiments showed the benefits and limits of these methods in terms of simplicity, precision, genericity and expressivity, while varying the level of aggregation of the input flow traces.

In addition, we have worked on our software-defined security framework, for enabling the enforcement of security policies in distributed cloud environments. This framework relies on the autonomic paradigm to dynamically configure and adjust these mechanisms to distributed cloud constraints, and exploit the software-defined logic to express and propagate security policies to the considered cloud resources [13]. In particular, we have investigated during Year 2017 the exploitability of unikernels to support our framework. Unikernels permit to build highly-constrained configurations limited to the strict necessary with a time-limited validity. We take benefits of their properties to reduce the attack exposure of cloud resources. We have formalized and integrated into our software-defined security framework, on-the-fly generation mechanisms of unikernel images that cope with security policy requirements. In that context, security mechanisms are directly integrated to the unikernel images at building time. A proof of concept prototype based on MirageOS was developed and the performance of such a software-based security strategy was evaluated through extensive series of experiments. We have also compared them to other regular virtualization solutions. Our results show that the costs induced by security mechanisms integration are relatively limited, and unikernels are well suited to minimize risk exposure.

7.3. Experimentation, Emulation, Reproducible Research

This section covers our work on experimentation on testbeds (mainly Grid'5000), on emulation (mainly around the Distem emulator), and on Reproducible Research.

7.3.1. Grid'5000 design and evolutions

Participants: Florent Didier, Arthur Garnier, Imed Maamria, Lucas Nussbaum [contact], Olivier Demengeon [SED], Teddy Valette [SED].

The team was again heavily involved in the evolutions and the governance of the Grid'5000 testbed.

7.3.1.1. Technical team management

Since the beginning of 2017, Lucas Nussbaum serves as the Grid'5000 *directeur technique* (CTO), managing the global technical team (9 FTE).

7.3.1.2. SILECS project

We are also heavily involved in the ongoing SILECS project, that aims at creating a new infrastructure on top of the foundations of Grid'5000 and FIT in order to meet the experimental research needs of the distributed computing and networking communities.

7.3.1.3. Promoting the testbed

In order to promote the testbed to the french devops and sysadmin community, we presented in [27] an overview of the testbed's capabilities.

7.3.1.4. Disk reservation

We contributed a new feature that will greatly help Big Data experimenters: the ability to reserve disks on nodes, in order to leave large datasets stored on nodes between nodes reservations.

7.3.1.5. Automated testing of the testbed

In order to ensure that all services remain functional, and that experimental results remain trustworthy and reproducible, we designed an infrastructure to automatically test the testbed and detect misconfigurations, regressions, uncontrolled hardware heterogeneity, etc. This work was described in [23] and later presented in [34].

7.3.1.6. Support for SDN experiments

We started the development of a tool to orchestrate SDN experiments on Grid'5000, combining KaVLAN and OpenVSwitch.

7.3.2. Emulation with Distem

Participants: Alexandre Merlin, Lucas Nussbaum [contact].

The ADT SDT project started in March. Initial work focused on improving the software developing infrastructure by adding automated regression tests on both correctness and performance. This should allow a new release in early 2018.

7.3.3. I/O access patterns analysis with eBPF

Participants: Abdulqawi Saif, Lucas Nussbaum [contact], Ye-Qiong Song.

In the context of Abdulqawi Saif's CIFRE PhD (with Xilopix), we explored the relevance of an emerging instrumentation technology for the Linux kernel, eBPF, and used it to analyze I/O access patterns of two popular NoSQL databases. A publication on this topic is expected in early 2018.

7.3.4. Performance study of public clouds

Participants: Souha Bel Haj Hassine, Lucas Nussbaum [contact].

We worked on clouds performance in the context of an ongoing collaboration with *CloudScreener*, a French startup founded in 2012 that has developed tools for cloud price and performance benchmarks and automated cloud recommendation to optimize the decision making process in the context of cloud computing. We designed methods and tools to do performance evaluation of public clouds focusing on (1) outlining performance variability over time; (2) identifying adverse strategies that might be deployed by cloud providers in order to vary the performance level over time.

7.3.4.1. Testbeds federation and collaborations in the testbeds community

The Fed4FIRE+ H2020 project started in January 2017 and will run until the end of September 2021. This project aims at consolidating the federation of testbeds in Europe of which Grid'500 is a member.

We are also active in the GEFI initiative that aims at building links between the US testbeds community (GENI) and their european (FIRE), japanese and brazilian counterparts. We participated in the annual GEFI meeting where gave two talks [33][34] and chaired the session on reproducibility.

7.3.4.2. Experimentation and reproducible research

In addition to the work already mentioned on testbed testing [23], [34], we worked on a survey of testbeds and their features for reproducible research [22]. We also gave several talks on reproducible research and testbeds at *École ARCHI* [5], *École RESCOM* [6], and Inria webinars on Reproducible Research [7].

7.4. Routing

7.4.1. NDN routing

Participants: Isabelle Chrisment [contact], Thomas Silverston, Elian Aubry.

As NDN relies on content names instead of host address it cannot rely on traditional Internet routing. Therefore it is essential to propose a routing scheme adapted for NDN. In [8] we have presented SRSC, our SDN-based Routing Scheme for CCN/NDN and its implementation. SRSC relies on the SDN paradigm. A controller is responsible to forward decisions and to set up rules into NDN nodes. So we have implemented SRSC into NDNx. We have deployed an NDN testbed within a virtual environment emulating a real ISP topology in order to evaluate the performances of our proposal with real-world experiments. We have demonstrated the feasibility of SRSC and its ability to forward Interest messages in a fully deployed NDN environment while keeping low overhead and computation time and high caching performances.

7.4.2. Energy-Aware and QoS Routing for Wireless Sensor Networks

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

The main research problems in the domain of routing data packets in a multi-hop wireless sensor network are the optimisation of the energy and the routing under multi-criteria QoS constraints (e.g., energy, reliability, delay, ...). To address these problems, we proposed, in the PhD thesis of E. Tiontsiou, two contributions. The first contribution is an optimal probabilistic energy-aware routing protocol, allowing to energy usage balancing. Comparing to the existing probabilistic routing protocols, our solution is based on the computation of the optimal probabilities by solving a linear programming problem. Our second contribution is an operator calculus algebra based multi-constrained routing protocol. It is fundamentally different from the existing solutions since it can simultaneously consider several constraints, instead of their combination.

7.5. Smart*: design, multi-modeling and co-simulation and supervision of mobile CPS/IoT

Participants: Laurent Ciarletta [contact], Ye-Qiong Song, Yannick Presse, Julien Vaubourg, Emmanuel Nataf, Petro Aksonenko, Virgile Dauge, Louis Viard, Florian Greff, Virginie Galtier, Thomas Paris.

Vincent Chevrier (former Maia team, Dep 5, LORIA) is a collaborator and the correspondant for the MS4SG/MECSYCO project, as well as Christine Bourjot (former MAIA team, Dep 5, LORIA).

Sylvain Contassot-Vivier (Dep 3, Loria) is a collaborator on the Grone project and is directing Virgile Daugé with Laurent Ciarletta.

Pierre-Etienne Moreau is a collaborator on the CEOS project and is directing Louis Viard with Laurent Ciarletta.

Virginie Galtier from CentraleSupélec is now a member of the Loria laboratory and will integrate the future Simbiot team (Systems of Interactive aMBient Intelligent ObjecTs).

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

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

We proposed the AA4MM meta-model [45] that solves the core challenges of multimodeling and simulation coupling in an homogeneous perspective. In AA4MM, we chose a multi-agent point of view: a multi-model is a society of models; each model corresponds to an agent and coupling relationships correspond to interaction between agents. In the MECSYCO-NG (formerly MS4SG, Multi Simulation for Smart Grids) project which involves some members of the former MAIA team, Madynes and EDF R&D on smart-grid simulation, we developed a proof of concepts for a smart-appartment case that serves as a basis for building up use cases, and we have worked on some specific cases provided by our industrial partner. We also collaborated with researchers from the Green UL laboratory.

In 2017 we worked on the following research topics:

- Overall assessment and evaluation of complex systems.
- Cyber Physical Systems and Smart *.

  We have continued the design and implementation of the Aetournos platform at Loria which will be part of the Creativ'Lab. The collective movements of a flock of flying communicating robots / UAVs, evolving in potentially perturbed environment constitutes a good example of a Cyber Physical System. Several projects have started during the last part of 2017. One of the emerging topic in this area is the safety of Mobile IoT/CPS with regards to their environment and users.

  - The Grone (Interreg) project involves partners from the 4 countries of the Grande Région (Centrale Supélec, LIST, Univ Luxembourg, Univ Liège, Fraunhofer IZFP to name a few). The main goal is to develop UAV based solution for the surveillance of industrial and agricultural sites and the exploration of GPS denied and underground environments. A PhD has been started in March 2017 (Systèmes cyber-physiques autonomes et communicants en milieux hostiles. Application à l'exploration par robots mobiles. Virgile Daugé).
  - and the CEOS (FUI22) project involving high profile companies (Thales C&S, EDF R&D, ENEDIS and Aéroport de Lyon) as well as academic partners (AOSTE2 Inria, ESIEE) and collaborating SMEs (RT@W, ADCIS, Alerion). This project focuses on the safety of UAV based monitoring solutions for OIV (Opérateurs d'Intéret Vital) infrastructures. A PhD has been started in November 2017 (Environnement de développement et d'analyse de propriétés pour des systèmes cyber-physiques mobiles. Louis Viard).

  The work on Software Defined Real-Time Mesh networks (Florian Greff's PhD CIFRE with Thales R&T) has given many results as he plans to defend his work in march 2018 [15], [39], [14].

  On more specific subject of innovative sensors for mobile and interactive IoT, a collaborative project with the KPI (Ukraine) university has been started with a projected PhD (Méthodes optimisées de calibration, d'alignement et algorithmes d'attitude avancés pour les systèmes de navigation inertiels fixés, Petro Aksonenko). Several papers have been published [9] [44] in 2017.
- (Very Serious) Gaming: Starburst Gaming. During some exploratory work, we have seen the potential of these Pervasive Computing ressources in the (Very Serious) Gaming area which led us to the Starburst Computing SATT projects in 2016 and 2017. A spin off has been founded in 2017 that is getting the licences for the resulting IP (the software is under the APP process at the time of this writing). Starburst is already involved in a AMI project with the Globlinz game studio and the lab and has officially been accepted in novembre 2017 and will be operational in 2018.
- Smart *: MS4SG / MECSYCO-NG has given us the opportunity to link simulations tools with a strong focus on FMI (Functional Mockup Interface) and network simulators (NS3/Omnet++). We have so far successfully applied our solution to the simulation of smart apartment complex and to combine the electrical and networking part of a Smart Grid. The AA4MM software is now MECSYCO and has seen constant improvements in 2017 thanks to the ressources provided by the MECSYCO-NG project in collaboration with EDF R&D (http://www.mecsyco.com), and the work of Thomas Paris and Julien Vaubourg.

  Starting from domain specific and heterogenous models and simulators, the MECSYCO suite allows for multi systems integration at several levels: conceptual, formal and software. A couple of visualization tools have been developed as proof of concepts both at run-time and post-mortem.

The technical report [43] has been extended into a journal paper under revision for a publication in 2018.

7.6. Quality-of-Service

7.6.1. Self-adaptive MAC protocol for both QoS and energy efficiency in IoT

Participants: Shuguo Zhuo, François Despaux, Ye-Qiong Song [contact].

The diversity of IoT applications implies the requirement of reliable yet efficient MAC solutions for supporting transmissions for various traffic patterns. We have mainly contributed to enhance the implementation of the high efficient traffic self-adaptive MAC protocols. As part of RIOT ADT project, our main achievements are the development of two MAC protocols lw-MAC and GoMacH [26]. lw-MAC is similar to X-MAC and ContikiMAC. It allows to introduce a first duty-cycled MAC into RIOT IoT protocol stack. GoMacH is a nearly optimal protocol that provides high reliability and throughput for handling various traffic loads in IoT. GoMacH seamlessly integrates several outstanding techniques. It adopts the phase-lock scheme to achieve low-power duty-cycled communication. It also utilizes a dynamic slots allocation scheme for providing accurate and instantaneous throughput boost. Furthermore, like in TSCH, GoMacH spreads its communications onto IEEE 802.15.4's 16 channels, leading to high reliability. GoMacH has been implemented in open source on RIOT OS, and has also been seamlessly integrated into IETF's 6LoWPAN/RPL/UDP stack as well as CCN-light. Experimental results on SAMR21-xpro test-beds and IoT-LAB verify the practicality of GoMacH and its capabilities for consistently providing high throughput, high delivery ratio, and low radio duty-cycle. They are both publically available on the RIOT open source github.

7.6.2. QoS and fault-tolerance in distributed real-time systems

Participants: Florian Greff, Laurent Ciarletta, Arnauld Samama [Thales TRT], Dorin Maxim, Ye-Qiong Song [contact].

The QoS must be guaranteed when dealing with real-time distributed systems interconnected by a network. Not only task schedulability in processors, but also message schedulability in networks should be analyzed for validating the system design. Fault-tolerance is another critical issue that one must take into account.

In collaboration with Thales TRT industrial partner as part of a CIFRE PhD work, we have developed a Software-Defined Real-time Network (SDRN) framework [14]. SDRN deals with the real-time flow allocation problem in mesh networks. The objective is to find a suitable path under delay constraint while allowing load balancing. For this purpose, combined online flow admission control and pathfinding algorithms have been developed on an SDN-like controller. At switch level, each output port is ruled by a credit-based weighted round robin, allowing isolation of flows. As a consequence, a freshly admitted flow will not influence existing flows, allowing incremental online admission of new flows. This approach has been applied to a RapidIO mesh network example and compared with the compositional performance analysis method. Numerical results clearly show the benefit of our proposal in terms of complexity and delay bound pessimism. In [15], Fault-tolerance issue in mesh networks has been addressed. In fact, one of the major advantages of a mesh topology is its ability to leverage the path redundancy in order to recover from link or node failures, through a flow reconfiguration process. However, one needs to ensure that hard real-time packets will keep being delivered on time during this transient reconfiguration period. Anticipating each possible fault is very complex and can result in a waste of network resource. Our contribution is the combination of an optimized content-centric source routing in nominal mode and a destination-tag flexible and scalable routing in transient recovery mode. We show the benefit of this approach in terms of flexibility and network resource utilization. Our method can ensure real-time properties enforcement even during the transient reconfiguration period. Algorithms have been developed to extend the SDRN flow allocation and routing methods in order to implement this hybrid fault-tolerant extension.

As part of Eurostars RETINA project, in the in-vehicle networking domain, we have focused on the evaluation of the worst-case response time of AVB traffic under time-aware shaper of TSN (time-sensitive networking). It is a hierarchical real-time scheduling problem, where a packet is scheduled by the credit-based shaper, priority and time-aware shaper (TDMA). We have proved that the eligible interval approach, developed for AVB, is still hold for TSN case. The worst case delay expression, as well as the feasibility condition are deduced. Our methods (analysis and simulation) are applied to an automotive use case, which is defined within the Eurostars RETINA project, and where both control data traffic and AVB traffic must be guaranteed. It has been shown that our delay bound is tight in single switch case [19].

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- Xilopix (Epinal, France):
  - Pay-per-use contract for the use of Grid'5000
  - Support contract for their use of Grid'5000 (define experimental requirements and plans)

8.2. Bilateral Grants with Industry

- CIFRE, Thales TRT (Paris, France):
  - CIFRE PhD (Florian Greff, supervised by Ye-Qiong Song and Laurent Ciarletta)
  - Dynamic reconfiguration and graceful degradation of distributed real-time applications over mesh networks
- CIFRE, Thales (Palaiseau, France):
  - CIFRE PhD (Pierre-Olivier Brissaud, supervised by Isabelle Chrisment and Jérôme François)
  - Anomaly detection in encrypted network traffic
- CIFRE, Orange Labs (Issy-Les-Moulineaux, France):
  - CIFRE PhD (Maxime Compastie, supervised by Olivier Festor and Rémi Badonnel)
  - Software-Defined Security for Distributed Cloud Infrastructures
- CIFRE, Orange Labs (Issy-Les-Moulineaux, France):
  - CIFRE PhD (Paul Chaignon, supervised by Olivier Festor and Jérôme François)
  - Monitoring of Software-Defined Networks
- CIFRE, Xilopix (Epinal, France):
  - CIFRE PhD (Abdulqawi Saif, supervised by Ye-Qiong Song and Lucas Nussbaum)
  - Open Science for the scalability of a new generation search technology
- CIFRE, Cynapsys Technologies (Paris, France):
  - CIFRE PhD (Haftay Gebreslasie Abreha, supervised by Michael Rusinowitch, Adel Bouhoula and Abdelkader Lahmadi)
  - Compressed and Verifiable Filtering Rules in Software-defined Networking

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. 6PO Research Region Lorraine and UL project

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

Funded by Region Lorraine and Université de Lorraine since 2013. Adel Belkadi (CRAN & LORIA) is co-directed by L. Ciarletta and Didier Theilliol (CRAN correspondant).

6PO ("Systèmes Cyber-Physiques et Commande Coopérative Sûre de Fonctionnement pour une Flotte de Véhicules sans Pilote") is a joint research project between the Loria and CRAN laboratories. As a part of the Aetournos ecosystem, it also aims at researching solutions for safe formation flying of collaborative UAVs seen as part of a collection of Cyber Physical Systems mixing computer science and automation solutions.

It is reinforced by a PhD grant from this federation that started in october 2014 (*Conception de méthodes de diagnostic et de tolérance aux fautes des systèmes multi-agents: Application à une flotte de véhicules autonomes*, Adel Belkadi) and has been successfully defended in october 2017.

This led to common publications, notably on the subjects of the robust control of a fleet or flock of UAVs (with or without leader, using agents paradigms and particle swarm optimisation [10] and [31]).

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

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

9.1.2. Hydradrone FEDER Région Lorraine project

Participants: Zhixiang Liu, Laurent Ciarletta [contact].

Feder funding

The Madynes team has been working on the Hydradrone project since July 2014. It started as a collaborative R&D initiative funded by *Région Lorraine* and is now FEDER funded. This project started as a joint work between Madynes and PEMA (*Pedon Environnement et Milieux Aquatiques*), an SME/VSE (small and medium size Entreprise, PME/TPE). The consortium now includes Alerion another VSE, a spinoff from Loria/UL.

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

- starting with an actual need for automated and remote operation of environmental sensing expressed by PEMA
- based on an hybrid UxV (Unmanned Air, Surface... Vehicle),
- some Cyber Physical bricks in coherence with the Alerion's concepts (ease of use, safety, autonomy)
- and an integration in the Information System of the company

PEMA, as an environmental company, provides the use cases and terrain (and business) validation, while Alerion is working on the integration and engineering of the solution.

This third year has been dedicated to the development of the surface controller for the Hydradrones along with the development of a new small version, and the integration of environmental sensors. The project has been extended towards the summer 2018 in order to finish the integration and tests.

9.1.3. Satelor AME Lorraine regional project

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

The Madynes team is involved in Satelor, a regional research and development project funded by the AME (Agence de Mobilisation Economique) of Lorraine (October 2013 – September 2017). The consortium includes academic (Univ. of Lorraine, Inria), medical (OHS) and industrial (Diatelic-Pharmagest (lead), ACS, Kapelse, Salendra, Neolinks) partners. It aims at developing innovative and easily deployable ambient assisted living solutions for their effective use in the tele-homecare systems. The Madynes team is mainly involved in the data collection system development based on wireless sensors networks and IoT technology. The first topic consists in defining the basic functions of the future SATEBOX – a gateway box for interconnecting in-home sensors to the medical datacenter, based on our previously developed MPIGate software. A beta-version prototype of the future Satebox gateway has been achieved. It now includes Zigbee wireless sensors, EnOcean battery-free sensors and Bluetooth Low Energy sensors. It provides a low-cost and easily deployable solution for the daily activity monitoring. After its first real-world deployment at a OHS hospital room, a second prototype testbed has been realized at one EHPAD including several rooms. The second topic is related to improve the data transfer reliability while still keep minimum energy consumption. This has led us to focus on the multi-hop mesh network topology with multi-constrained QoS routing problem (PhD thesis of Evangelia Tsiontsiou). The third topic is UWB-based indoor localization and its use for tracking and detecting falls of the elderlies. Experiments have shown a great benefice of multi-sensor fusion (e.g. localization + accelerometer) for increasing the detection accuracy.

9.2. National Initiatives

9.2.1. ANR

9.2.1.1. ANR BottleNet

Participants: Isabelle Chrisment [contact], Thibault Cholez, Vassili Rivron.

The Quality of Experience (QoE) when accessing the Internet, on which more and more human activities depend on, is a key factor for today's society. The complexity of Internet services and of user's local connectivity has grown dramatically in the last years with the proliferation of proxies and caches at the core and access technologies at the edge (home wireless and 3G/4G access), making it difficult to diagnose the root cause of performance bottlenecks. The objective of BottleNet is to deliver methods, algorithms, and software systems to measure end-to-end Internet QoE and to diagnose the cause of experienced issues. The result can then be used by users, network and service operators or regulators to improve the QoE.

The ANR BottleNet project (https://project.inria.fr/bottlenet) started in February 2016. It involves many partners in the field of computer networks and QoE: Inria Muse and Diana teams, Lille1 University, Telecom Sud-Paris, Orange, IP-Label. The objective of BottleNet is to deliver methods, algorithms, and software systems to measure Internet QoE and diagnose the root cause of poor Internet QoE. Our goal calls for tools that run directly at users' devices. We plan to collect network and application performance metrics directly at users' devices and correlate them with user perception to model Internet QoE, and to correlate measurements across users and devices to diagnose poor Internet QoE. This data-driven approach is essential to address the challenging problem of modeling user perception and of diagnosing sources of bottlenecks in complex Internet services. BottleNet will lead to new solutions to assist users, network and service operators as well as regulators in understanding Internet QoE and the sources of performance bottleneck.

9.2.1.2. ANR Doctor

Participants: Thibault Cholez [contact], Xavier Marchal, Daishi Kondo, Olivier Festor.

The DOCTOR project http://www.doctor-project.org is an applied research project funded by the French National Research Agency (ANR), grant <ANR-14-CE28-000>, and supported by the French Systematic cluster. The project started on December 2014 for three years plus one year of extension (2018) to align the scientific production with the budget consumption. It involves five partners specialized in network monitoring and security: Orange Labs (lead), Thales, Montimage, Université de technologie de Troyes and LORIA/CNRS. The DOCTOR project advocates the use of virtualized network equipment (Network Functions Virtualization), to enable the co-existence of new Information-Centric Networking stacks (e.g.: Named-Data Networking) with IP, and the progressive migration of traffic from one stack to the other while guaranteeing the good security and manageability of the network. Therefore in DOCTOR, the main goals of the project are: (1) the efficient deployment of NDN as a virtualized networking environment; (2) the monitoring and security of this virtualized NDN stack.

This year, we focused on the second workpackage dedicated to security. We did a joint work with UTT investigating the impact on the Content Poisoning Attack on the NDN architecture [21]. We also wrote a book chapter about our use of NDN and NFV technologies to deploy an NDN network while providing advanced monitoring and security functions [35].

We also improved our HTTP/NDN gateway that will be soon released for the community and which design and evaluation will be submitted in a journal.

The next (and last) year of the project will be dedicated to the orchestration of our virtualized NDN architecture to manage its performance and security, and to the deployment of a testbed carrying real user traffic.

9.2.1.3. FUI HUMA (01/09/2015-31/08/2018)

Participants: Giulia de Santis, Soline Blanc, Sofiane Lagraa, Jérôme François [contact], Abdelkader Lahmadi, Isabelle Chrisment.

The HUMA project (*L'HUmain au cœur de l'analyse de données MAssives pour la sécurité*) is funded under the national FUI Framework (Fonds Unique Interministeriel) jointly by the BPI (Banque Publique d'Investissement) and the Région Lorraine. It has been approved by two competitive clusters: Systematic and Imaginove. The consortium is composed of three academic (ICube, Citi, Inria) and five industrial (Airbus Defence and Space, Intrinsec, Oberthur, Wallix, Sydo) partners. The leader is Intrinsec.

This project targets the analysis of Advanced Persistent Threat. APT are long and complex attacks which thus cannot be captured with standard techniques focused on short time windows and few data sources. Indeed, APTs may last for several months and involve multiple steps with different types of attacks and approaches. The project will address such an issue by leveraging data analytics and visualization techniques to guide human experts, which are the only one able to analyze APT today, rather than targeting a fully automated approach.

In 2017, our contribution focused on defining a graph-mining technique to discover dependencies among security events clustering techniques in order to group individual events into a common one. We applied our technique to darknet data as shown in section 7.2.1. In addition, we also start the modeling of an attacker process by considering the first phase of APT, *i.e.* the reconnaissance phase by analyzing scanning activities using Hidden Markov Model (7.2.1). We also technically contribute to the definition of APT scenarios by providing a very stealthy scanning approach (Wiscan described in 7.1.2). Finally, from a project management point of view, Inria is in charge of leading the work-package related to data analytics technique for analyzing security probe events.

9.2.1.4. Inria-Orange Joint Lab

Participants: Jérôme François [contact], Rémi Badonnel, Olivier Festor, Maxime Compastié, Paul Chaignon.

The challenges addressed by the Inria-Orange joint lab relate to the virtualization of communication networks, the convergence between cloud computing and communication networks, and the underlying software-defined infrastructures. This lab aims at specifying and developing a GlobalOS (Global Operating System) approach as a platform or a software infrastructure for all the network and computing resources required by the Orange network operator. Our work, started in November 2015, concerns in particular monitoring methods for software-defined infrastructures, and management strategies for supporting software-defined security in multi-tenant cloud environments. We have specified a management framework dedicated to cloud software-defined security. It relies on on-the-fly generation and execution of unikernels in order to build highly-constrained configurations. The solution has been evaluated through extensive series of experiments, based on a proof-of-concept prototype using MirageOS. Results show that the costs induced by security mechanisms integration are relatively limited, and unikernels are well suited to minimize risk exposure.

9.2.1.5. ANR FLIRT

Participants: Olivier Festor [contact], Rémi Badonnel, Thibault Cholez, Jérôme François, Abdelkader Lahmadi, Laurent Andrey.

FLIRT (Formations Libres et Innovantes Réseaux & Télécom) is an applied research project leaded by the Institut Mines-Télécom, for a duration of 4 years. It includes 14 academic partners (engineering schools including Telecom Nancy), 3 industrial partners (Airbus, Nokia Group and Orange), 2 innovative startups (the MOOC agency, and Isograd), as well as 3 professional or scientific societies (Syntec Numérique, Unetel, SEE). The project objective is to build a collection of 10 MOOCs (Massive Open Online Courses) in the area of networks and telecommunications, 3 training programmes based on this collection, as well as several innovations related to pedagogical efficiency (such as virtualization of practical labs, management of student cohorts, and adaptative assessment). The Madynes team is leading a working group dedicated to the building of a MOOC on network and service management. This MOOC, whose first session will open end of 2018, covers the fundamental concepts, architectures and protocols of the domain, as well as their evolution in the context of future Internet, and includes practical labs and exercises using widely-used tools and technologies.

9.2.2. Technological Development Action (ADT)

9.2.2.1. ADT UASS

The goal of this ADT provides assistance in developing the Aetournos platform to help in the UAV Challenge Medical Express. Through this ADT, funded by Inria, Raphaël Cherfan has coordinated students work on the platform and tutored the Aetournos team for the 2016 Outback Joe Search and Rescue / Medical Express Challenge, and help in the design and buidling of a novel Hybrid UAV.

9.2.2.2. ADT VERTEX

This ADT started in 2016 and will end on 2018. The Madynes project is a major partner funded at the level of 120k€. ADT VERTEX built upon the foundations of the Grid'5000 testbed aims to reinforce and extend it towards new use cases and scientific challenges. Several directions are being explored: networks and Software Defined Networking, Big Data, HPC, and production computation needs. Previously developed prototypes are also being consolidated, and the necessary improvements to user management and tracking are also being performed.

9.2.2.3. ADT SDT

Built on the Distem emulator, that enables the creation of virtual experimental environments from clusters of homogeneous machines, this project aims at enlarging the scope of use of Distem to additional fields: *Software Defined Networking*, *Named Data Networking*, *Big Data*. In addition, we will explore *temporal dilation* as a technique to study future infrastructures.

The project started in 2017 and will end in 2019.

9.2.2.4. ADT RIOT

RIOT ADT is a multi-site project with Infine and Madynes teams, which started in December 2016 for a duration of two years. The high-level objective is to (1) contribute open source code, upstream, to the RIOT code base, (2) coordinate RIOT development within Inria, with other engineers and researchers using/developing RIOT, (3) coordinate RIOT development outside Inria, help maintain the RIOT community at large (see http://www.riot-os.org and http://www.github.com/RIOT-OS/RIOT) which aims to become the equivalent of Linux for IoT devices that cannot run Linux because of resource constraints.

This year MADYNES team has mainly contributed to the efficient MAC layer protocol implementation issues. We have built a general MAC protocol module (gnrc mac module) for providing critical development tools for MAC protocol developers in the RIOT community. Based on these generic functions, we have developed two duty-cycled MAC protocols lw-MAC and GoMacH which are above IEEE802.15.4. lw-MAC is a single channel MAC protocol that has similar principle of X-MAC and ContikiMAC. GoMacH [26] is a traffic-adaptive multi-channel MAC protocol for IoT which exhibes low power consumption and high throughput performance. Both are integrated into the RIOT IoT protocol stack and merged into RIOT master branch. They are publically available in RIOT open source github.

9.2.2.5. ATT AMICS

The ATT AMICS is run in cooperation with the High Security Lab (HSL). The goal is to develop a customizable security analytics stack as a service. The added value of the HSL is to cross-correlate customer data with Internet probes hosted at HSL collecting tons of security data. Indeed, the basic service provided to potential customer is a VPN on top of which custom modules can be added. In 2017, we setup the VPN elements and also developed a flexible framework for security analysis. Different moddules have already been defined and implemented: blacklists aggregators to gather continuously information from third parties providing blacklists, real-time verification of traffic going through the VPN using blacklists, real-time detection of IP spoofing by correlating user traffic with HSL darknet traffic and real-time detection of customer hosts infected by a malware.

9.2.3. Inria Project Lab

9.2.3.1. IPL BetterNet

Participants: Isabelle Chrisment [contact], Thibault Cholez, Vassili Rivron, Lakhdar Meftah [University of Lille].

The Inria Project Lab BetterNet (https://project.inria.fr/betternet) has been launched in October 2016. Its goal is to build and deliver a scientific and technical collaborative observatory to measure and improve the Internet service access as perceived by users. We will propose new original user-centered measurement methods, which will associate social sciences to better understand Internet usage and the quality of services and networks. Tools, models and algorithms will be provided to collect data that will be shared and analyzed to offer a valuable service to scientists, stakeholders and civil society.

The Madynes team leads this IPL and in particular Isabelle Chrisment who coordinates the project.

In 2017, the main activities of the project focused on federating Inria's monitoring tools (APISENSE, Fathom, Hostview, ACQUA) and building our open measurement platform for acquiring data.

Lakhdar Meftah, a shared PhD student with the SPIRALS team (Inria/University of Lille) has worked on a privacy preservation scheme using data dissemination that introduces an a priori data anonymization and improves user privacy without compromising the overall quality of the crowdsourced dataset.

9.2.3.2. IPL Discovery

Participant: Lucas Nussbaum [contact].

To accommodate the ever-increasing demand for Utility Computing (UC) resources, while taking into account both energy and economical issues, the current trend consists in building larger and larger Data Centers in a few strategic locations. Although such an approach enables UC providers to cope with the actual demand while continuing to operate UC resources through centralized software system, it is far from delivering sustainable and efficient UC infrastructures for future needs.

The DISCOVERY initiative aims at exploring a new way of operating Utility Computing (UC) resources by leveraging any facilities available through the Internet in order to deliver widely distributed platforms that can better match the geographical dispersal of users as well as the ever increasing demand. Critical to the emergence of such locality-based UC (also referred as Fog/Edge Computing) platforms is the availability of appropriate operating mechanisms. The main objective of DISCOVERY is to design, implement, demonstrate and promote a new kind of Cloud Operating System (OS) that will enable the management of such a large-scale and widely distributed infrastructure in an unified and friendly manner.

The consortium is composed of experts in the following research areas: large-scale infrastructure management systems, networking and P2P algorithms. Moreover, two key network operators, namely Orange and RENATER, are involved in the project.

By deploying and using a Fog/Edge OS on backbones, our ultimate vision is to enable large parts of the Internet to be hosted and operated by its internal structure itself: a scalable set of resources delivered by any computing facilities forming the Internet, starting from the larger hubs operated by ISPs, governments and academic institutions, to any idle resources that may be provided by end users.

MADYNES contributes to the DISCOVERY IPL on the networking axis. A CIFRE PhD with Orange is expected to start at the beginning of 2018.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. Fed4Fire+ (2017-2022)

Title: Federation for FIRE Plus

Program: H2020

Duration: January 2017 - December 2021

Coordinator: Interuniversitair Micro-Electronicacentrum Imec VZW

Partners:

Universidad de Malaga

National Technical University of Athens - NTUA

The Provost, Fellows, Foundation Scholars & the other members of board of the College of the Holy & Undivided Trinity of Queen Elizabeth Near Dublin

Ethniko Kentro Erevnas Kai Technologikis Anaptyxis

GEANT LImited

Institut Jozef Stefan

Mandat International Alias Fondation Pour la Cooperation Internationale

Universite Pierre et Marie Curie - Paris 6

Universidad De Cantabria

Fundacio Privada I2CAT, Internet I Innovacio Digital A Catalunya

EURESCOM-European Institute For Research And Strategic Studies in Telecommunications GMBH

Nordunet A/S

Technische Universitaet Berlin

Instytut Chemii Bioorganicznej Polskiej Akademii Nauk

Fraunhofer Gesellschaft zur Foerderung Der Angewandten Forschung E.V.

Universiteit Van Amsterdam

University of Southampton

Martel GMBH

Atos Spain SA

Institut National de Recherche en Informatique et automatique

Inria contact: David Margery (for MADYNES: Lucas Nussbaum)

Fed4FIRE+ is a successor project to Fed4FIRE. In Fed4FIRE+, we more directly integrate Grid'5000 into the wider eco-system of experimental platforms in Europe and beyond using results we developped in Fed4FIRE. We will also provide a generalised proxy mechanisms to allow users with Fed4FIRE identities to interact with services giving access to different testbeds but not designed to support Fed4FIRE identities. Finally, we will work on orchestration of experiments in a federation context. Fed4FIRE+ was prepared in 2016, and has started January 1st, 2017.

9.3.2. Collaborations in European Programs, Except FP7 & H2020

9.3.2.1. RETINA

Program: Eurosatrs-2

Project acronym: RETINA

Project title: Real-Time support for heterogenous networks in automotive applications

Duration: April 2016 - March 2018

Coordinator: TCN (Time critical networks)

Other partners: TCN (Sweden), Alkit (Sweden), Viktoria (Sweden), TNO (Netherlands), Scuola Superiore Sant'Anna (Italy), Evidence (Italy), University of Lorraine (France)

Abstract: The project will develop integrated software tools to predict, simulate, test and support real-time communication in heterogeneous vehicular networks. The tool set will allow SMEs and larger industry to design, develop and evaluate time-critical applications such as advanced safety systems and autonomous vehicles. This will put high requirements on both in-vehicle infrastructure, as well as vehicle-to-vehicle and vehicle-to infrastructure utilizing the next generation of mobile networks for ITS.

9.4. International Initiatives

9.4.1. Inria Associate Teams Not Involved in an Inria International Labs

9.4.1.1. IoT4D

Title: Internet of Things for Developping countries

International Partner (Institution - Laboratory - Researcher):

UY (Cameroon) - MASECNeSS - Thomas DJOTIO NDIE

Start year: 2016

See also: https://team.inria.fr/iot4dc/

Our goal is to connect wireless sensors networks (WSN) to the Internet through gateways. WSN should have several accessible gateways (depending on the size and quality of service needed) and gateways should be used by several wireless sensors networks. This is an optimization problem in a peculiar context featuring unreliable communications and equipments that are easily disturbed by environment .

9.4.1.2. Masdin

Title: MAnagement of Software-Defined INfrastructure

International Partner (Institution - Laboratory - Researcher):

University of Luxembourg (Luxembourg) - SnT (Interdisciplinary Centre for Security, Reliability and Trust) - Radu State

Joint publications: [25], [12], [16]

Start year: 2016

See also: https://project.inria.fr/masdin

Networking is deeply evolving with the advent of new paradigms making the network more configurable and more dynamic. In particular, SDN (Software-Defined Network) consists in splitting the control plane and the data plane. A SDN-enabled switch is so only viewed as a specialized device in forwarding data traffic while a logically centralized controller exposes interfaces to services and applications strengthening their coupling. Hence, network is not only a medium of communication but a software component. In the same context, NFV (Network Function Virtualization) promotes the virtualization of all kinds of network functions (router, load-balancer, firewall. . .) on commodity server, a server in a cloud. These technologies are deeply changing networking principle by allowing a high flexibility in network management. The new features provided by these concepts will thus allow to reinvent the network management in all its areas, especially for network monitoring and provisioning. In addition, even more recent propositions argue for a finer granularity applying the programmability idea of SDN (working at flow level) to packet processing level by promoting the definition of a common language like P4 to reconfigure any switch at low level (vendor independent). The original goal of the associate team is to explore co-jointly this research area through four directions: Monitoring of NFV- and SDN-enabled networks, investigating the integration of data analytics as virtualized functions in virtual networks, security of SDN networks, service chain composition, programming packet processing with P4 and other equivalents. ICN (Information Centric Networking) is also an important topic which is addressed in the team, especially regarding performance (with SDN) and security.

Furthermore, management of blockchain has been set as a new research topic to be focused in the team at the end of 2016. In the scope of network management, our objective is to design monitoring and orchestration methods for blockchain. In particular, we want to assess the relationships and impact between blockchain and network performance. We will have to define proper metrics to catch meaningful data to be analyzed. Moreover, a blockchain technology is by nature without authority (except in the private case), configuration requires thus to enforce some collaboration between nodes.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

Rémi Badonnel: IEEE/IFIP International Symposium on Integrated Network Management (IEEE/IFIP IM 2017), IFIP International Conference on Autonomous Infrastructure, Management and Security (IFIP AIMS 2017), IEEE/IFIP International Network Operations and Management Symposium (IEEE/IFIP NOMS 2018).

Lucas Nussbaum: 4th International Workshop on Reproducibility in Parallel Computing (REPPAR 2017).

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

Isabelle Chrisment was a TPC co-chair of the 2nd IEEE/IFIP Workshop on Analytics for Network and Service Management (AnNet 2017). She was member of the steering committee for RESSI'17 (Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information).

Rémi Badonnel is a TPC co-chair for the Third IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2018).

Jérôme François was a co-chair of the 3rd IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT).

Lucas nussbaum was a co-chair of the *High Performance Computing in/with the Cloud* track at 9th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2017).

10.1.2.2. Member of the Conference Program Committees

Rémi Badonnel: IFIP/IEEE International Conference on Network and Service Management (IFIP/IEEE CNSM 2017) ; IEEE Conference on Network Softwarization (IEEE NetSoft 2017) ; IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM 2017) ; IFIP International Conference on Autonomous Infrastructure, Management and Security (IFIP AIMS 2017) ; IEEE Global Information Infrastructure and Networking Symposium (IEEE GIIS 2017) ; Asia-Pacific Network Operations and Management Symposium (APNOMS 2017) ; IEEE International Conference on Communications (IEEE ICC - SAC 2017).

Olivier Festor: IFIP/IEEE International Conference on Network and Service Management (IFIP/IEEE CNSM 2017) ; IEEE Conference on Network Softwarization (IEEE NetSoft 2017) ; IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM 2017) ; IFIP International Conference on Autonomous Infrastructure, Management and Security (IFIP AIMS 2017) ; IFIP Networking 2017.

Abdelkader Lahmadi: IEEE Conference on Network Softwarization (IEEE NetSoft 2017) ; IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM 2017) ; Asia-Pacific Network Operations and Management Symposium (APNOMS 2017) ; 1st Cyber Security in Networking Conference (CSNET 2017).

Jérôme François: IEEE Conference on Network Softwarization (IEEE NetSoft 2017) ; IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM 2017) ; Asia-Pacific Network Operations and Management Symposium (APNOMS 2017) ; IEEE Global Information Infrastructure and Networking Symposium (IEEE GIIS 2017) ; Principles, Systems and Applications of IP Telecommunications (IPTComm'17); IFIP/IEEE International Workshop on Management of SDN and NFV Systems (IFIP/IEEE ManSDN 2017).

Thibault Cholez: IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT 2017); 4th ACM Conference on Information-Centric Networking: Demos and Posters tracks (ICN 2017).

Lucas Nussbaum: 4th International Workshop on Computer and Networking Experimental Research Using Testbeds (CNERT'2017) ; 26th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'2017) ; 23nd IEEE International Conference on Parallel and Distributed Systems (ICPADS'2017).

Isabelle Chrisment: IFIP International Conference on Autonomous Infrastructures, Management and Security (IFIP AIMS'17) ; Rencontres Francophones sur la Conception de Protocoles, l'évaluation de Performance et l'Expérimentation Aspects Algorithmiques de Télécommunications (CoResl'17) ; IEEE/IFIP International Symposium on Network Operations and Management (IFIP/IEEE IM'17).

Ye-Qiong Song: IEEE International Workshop on Factory Communication Systems (WFCS 2017); IEEE International Conference on Communications and Networking (ComNet 2017) ; IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2017) ; 25th International Conference on Real-Time Networks and Systems (RTNS 2017) ; IEEE Clobecom 2017; ICOST 2017; IEEE RTCSA 2017.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

Rémi Badonnel is Associate Editor for the Wiley International Journal of Network Management (IJNM), and serves as a Guest Editor for a Special Issue on Management of SDN/NFV-based Systems in the same journal.

Jérôme François serves as a Guest Editor for a Special Issue on Security for Emerging Open Networking Technologies in Wiley International Journal of Network Management (IJNM).

Ye-Qiong Song is an Associate Editor for the Elsevier Computers and Electrical Engineering journal, and for the Journal of Multimedia Information System.

10.1.3.2. Reviewer - Reviewing Activities

The following reviews for journals has been made by team members:

Rémi Badonnel: IEEE Transactions on Network and Service Management (IEEE TNSM), Springer Journal of the Network and Systems Management (JNSM), Wiley International Journal of Network Management (IJNM), IEEE Communications Magazine (COMMAG), Elsevier Journal on Computer Communications (COMCOM), Elsevier Journal on Communication Networks (COMNET), Elsevier Journal on Computers and Security (COSE).

Olivier Ferstor: Elsevier Computers & Security.

Abdelkader Lahmadi: IEEE Transactions on Network and Service Management (IEEE TNSM), Springer Journal of the Network and Systems Management (JNSM), Wiley International Journal of Network Management (IJNM), International Journal of Distributed Sensor Networks (IJDSN), IEEE Communications Magazine (COMMAG).

Jérôme François: IEEE Communications Magazine (COMMAG), Wiley International Journal of Network Management (IJNM).

Thibault Cholez: Wiley International Journal of Network Management (IJNM), Elsevier Journal on Communication Networks (COMNET).

Lucas Nussbaum: PLOS ONE ; Springer Journal of Internet Services and Applications (JISA) ; International Journal of Grid and Utility Computing (IJGUC) ; IEEE Transactions on Services Computing (TSC).

Isabelle Chrisment: IEEE Transactions on Network and Service Management (IEEE TNSM), IEEE Communications Magazine (COMMAG). Elsevier Journal Computer Communications (COMCOM)

Ye-Qiong Song: Elsevier Computers and Electrical Engineering journal, IEEE Transactions on Industrial Informatics, IEEE Communications surveys and tutorials.

10.1.4. Invited Talks

Jérôme François:

- IRTF NMRG (IETF 100), Singapore: "Network traffic analysis for encrypted traffic and security monitoring"
- 7th annual Inria@SiliconValley workshop, Berkeley, CA, USA: panelist on "Blockchain Technology for Cybersecurity and Social Impact" and presenter in session "Scaling up for IoT"
- Annual CODE event of the Universität der Bundeswehr, Munich, Germany: panelist on "Smart Atttacks requires smart defence"

Lucas Nussbaum:

- École ARCHI 2017: "Experimenting on Architectures for High Performance Computing"
- Reproducible Research Webinars: "Testbeds in Computer Science"
- École RESCOM 2017: "Scaling Your Experiments"

Vassili Rivron:

- CERReV/Université de Caen Normandie Conference on *Les services gratuits du web entre empowerment et hégémonie : contradictions et régulations de l'économie collaborative*, "Sites d'information et bloqueurs de publicité : intermédiaires de l'auto-régulation publicitaires dans le champ journalistique", March 2017.
- SHS Seminar in Loria, "News-sites and adblockers : intermediaries of advertising self-regulation in the field of journalism", in collaboration with Thibault Cholez, June 2017.

10.1.5. Scientific Expertise

Abdelkader Lahmadi served as a member of the Selection Committee of the 2017 ComSoc Student Competition "Communications Technology Changing the World".

Jérôme François serves as reviewer for ANRT to evaluate a CIFRE PhD proposition and as reviewer for ANR.

Yeqiong Song serves as reviewer for ANRT to evaluate a CIFRE PhD proposition and as reviewer for ANR.

10.1.6. Research Administration

Abdelkader Lahmadi is a member of the CDT of Inria Nancy Grand Est.

Jérôme François is a member of the Horizon Startup local committee in Nancy Grand Est.

Isabelle Chrisment is a member of :

- AFNIC's scientific council
- scientific pole AM2I (Automatique, Mathématiques, Informatique et leurs Interaction) at Université de Lorraine
- COMIPERS at Inria Nancy Grand Est.
- CMI (Commission de la Mention Informatique), part of the doctoral school IAEM.

She also served as a member of the working group "Plan Stratégique Scientifique Inria".

Olivier Festor is member of the Scientific Council of Telecom Sud Paris. Olivier Festor is leading the IFIP TC6 Working Group 6.6 : Network and Service Management. He is also in charge of the CERI initiative between France and Germany.

Yeqiong Song is head of Department 3 of LORIA.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Olivier Festor is the Director of the TELECOM Nancy Engineering School.

Rémi Badonnel is heading the Internet Systems and Security specialization of the 2nd and 3rd years at the TELECOM Nancy engineering school, and is coordinating the Security Pathway Program at the same school, elaborated in the context of the International Master of Science in Security of Computer Systems built with the Mines Nancy school.

Laurent Ciarletta is co-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).

Team members are teaching the following courses:

Rémi Badonnel 242 hours - L3, M1, M2 - Networks, Systems and Services, Software Design and Programming, Cloud Computing, Network and Security Management - TELECOM Nancy, Université de Lorraine

Abdelkader Lahmadi 280 hours - L3, M1, M2 - Real time and Embedded Systems Programming, Distributed Systems and Algorithms, Green IT, Algorithms and Advanced Programming - ENSEM Engineering School

Yeqiong Song 200 hours - L3, M1, M2 - Green IT, Algorithms and Advanced Programming, Databases networking - ENSEM Engineering School

Jérôme François 70 hours - M1, M2 -Network security, Big Data - TELECOM Nancy, Université de Lorraine, University of Lorraine

Thibault Cholez 300 hours - L3, M1, M2 - Techniques and Tools for Programming, Computer Networks, Object-Oriented Programming, Network Services, Constraint development on small Connected Objects, Mobile applications and Internet of Things, Project Management - TELECOM Nancy, Université de Lorraine, University of Lorraine

Isabelle Chrisment 220 hours -L3, M1, M2 -C and Shell Programming, Computer Networking, Operating Systems, Network Security. - TELECOM Nancy, Université de Lorraine

E-learning

MOOC: Thibault Cholez, Supervision de réseaux et services (concept clés avec SNMP), 1 semaine (5 leçons), FUN, Université de Lorraine, Ingénieur, formation initiale et continue, ouverture en janvier 2018.

MOOC: Rémi Badonnel, Laurent Andrey, Supervision de réseaux et services (monitoring avec Nagios), 1 semaine (5 leçons), FUN, Université de Lorraine, Ingénieur, formation initiale et continue, ouverture en janvier 2018.

MOOC: Olivier Festor, Abdelkader Lahmadi, Supervision de réseaux et services (instrumentation avec JMX), 1 semaine (3 leçons), FUN, Université de Lorraine, Ingénieur, formation initiale et continue, ouverture en janvier 2018.

MOOC: Jérôme François, Supervision de réseaux et services (évolution des protocoles), 1 semaine (4 leçons), FUN, Université de Lorraine, Ingénieur, formation initiale et continue, ouverture en janvier 2018.

10.2.2. Supervision

PhD: Wazen Shbair, *Service-Level Monitoring of HTTPS Traffic* [1] defended on May 3rd 2017, University of Lorraine, supervised by Isabelle Chrisment and Thibault Cholez.

PhD: Julien Vaubourg, *Intégration de modèles de réseaux IP à un multi-modèle DEVS, pour la co-simulation de systèmes cyber-physiques* [2], defended in April 2017, Université de Lorraine, supervised by Vincent Chevrier and Laurent Ciarletta.

PhD: Evangelia Tsiontsiou, *Multi-constrained QoS Routing and Energy Optimization in Wireless Sensor Networks*, defended on December 15th 2017, University of Lorraine, supervised by Ye-Qiong Song and Bernardetta Addis.

PhD: Patrick-Olivier Kamgueu, *Configuration Dynamique et Routage pour l'Internet des Objets*, defended on December 18th 2017, Université de Yaoundé & Universiité de Lorrain, supervised by Olivier Festor, Emmanuel Nataf and Thomas Djotio

PhD: Elian Aubry, *Protocole de routage pour l'architecture NDN*, defended on December 19th 2017, University of Lorraine, supervised by Isabelle Chrisment and Thomas Silverston

PhD in progress: Thomas Paris, *Mo, délisation de systèmes complexes par composition*, since September 2015, supervised by Vincent Chevrier and Laurent Ciarletta.

PhD in progress: Maxime Compastie, *Software-Defined Security for the Cloud*, since December 2015, supervised by Olivier Festor and Rémi Badonnel.

PhD in progress: Florian Greff, *QoS and fault-tolerance of distributed real-time systems over mesh networks*, since Feb. 2015, supervised by Ye-Qiong Song and Laurent Ciarletta.

PhD in progress: Nicolas Schnepf, *Orchestration and Verification of Security Functions for Smart Environments*, since October 2016, supervised by Stephan Merz, Rémi Badonnel and Abdelkader Lahmadi.

PhD in progress: Giulia De Santis, *Data Analytics for Security*, since October 2015, supervised by Olivier Festor, Abdelkader Lahmadi and Jérôme François.

PhD in progress: Paul Chaignon, *Mécanismes de supervision de la sécurité dans un réseau programmable de type SDN/NFV*, since November 2015, supervised by Olivier Festor, Kahina Lazri and Jérôme François.

PhD in progress: Xavier Marchal, *Secure operation of virtualized Named Data Networks*, since December 2015, supervised by Olivier Festor and Thibault Cholez.

PhD in progress: Salvatore Signorello, *A multifold approach to address the security issues of stateful forwarding mechanisms in Information- Centric Networks*, since December 2014, supervised by Olivier Festor, Jérôme François and Radu State.

PhD in progress: Abdulqawi Saif, *Open Science for the scalability of a new generation search technology*, since December 2015, supervised by Ye-Qiong Song and Lucas Nussbaum.

PhD in progress: Pierre-Olivier Brissaud, *Anomaly detection in encrypted traffic*, since July 2016, supervised by Isabelle Chrisment, Jérôme François and Thibault Cholez.

PhD in progress: Petro Aksonenko, *Positionnement robuste pour véhicules autonomes à base de fusion de données de capteurs reposant sur les systèmes de navigation inertielle*, since October 2016, supervised by Patrick Henaff (Biscuit, Dep 5, loria), Vadim Avrutov (Kiev Polytechnic institute in Urkaine) and Laurent Ciarletta.

PhD in progress: Lakhdar Meftah, *Cartography of the quality of experience for mobile internet access*, since November 2016, supervised by Romain Rouvoy and Isabelle Chrisment.

PhD in progress: Haftay Gebreslasie Abreha, *Compressed and Verifiable Filtering Rules in Software-defined Networking*, since Octobrer 2017, supervised by Michael Rusinowitch, Abdelkader Lahmadi and Adel Bouhoula.

PhD in progress: Mingxiao Ma, *Cyber-physical systems defense through smart network configuration*, since December 2017, supervised by Isabelle Chrisment and Abdelkader Lahmadi.

PhD in progress: Louis Viard, *Environnement de développement et d'analyse de propriétés pour des systèmes cyber-physiques mobiles*, since November 2017, supervised by Pierre-Etienne Moreau and Laurent Ciarletta.

10.2.3. Juries

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

- Maryam Barshan, PhD in Computer Science from Ghent University, Belgium. Title: Cloud Resource Provisioning and Bandwidth Management in Media-Centric Networks, August 2017 – (Rémi Badonnel as reviewer).

- Jose Jair Cardoso de Santanna, PhD in Computer Science from University of Twente, The Netehrlands. Title: DDOS-as-a-Service - Investigating Booter Websites, November 2017 – (Olivier Festor as reviewer).
- Amina Boubendir, PhD in Computer Science from TELECOM ParisTech, France. Title: Flexibility and Dynamicity for Open Network-as-a-Service : From Architecture Modeling to Deployment, March 2017 – (Olivier Festor as reviewer).
- Merve Sahin, PhD in Computer Science from TELECOM ParisTech, France. Title: Understanding Telephony Fraud as an Essential Step to Better Fight It, September 2017 – (Olivier Festor as reviewer).
- Christian Hammerschmidt, PhD in Computer Science from the University of Luxembourg, Luxembourg Title: Learning Finite Automata via Flexible State-Merging and Applications in Networking – (Jérôme François as reviewer).
- Pascal Thubert, PhD in Computer Science from IMT Atlantique - Bretagne -Pays de Loire, France. Title: Converging over Deterministic Networks for an Industrial Network, March 2017 – (Isabelle Chrisment as reviewer).
- Yoann Bertrand, PhD in Computer Sciencce from Université Côte d'Azur, France. Title: Access control policies and companies data transmission management, March 2017 – (as examiner).
- Eric Asselin, Phd in Computer Science from Université de Toulouse, France. Title: Système de détection d'intrusion adapté au système de communication aéronautique ACARS, June 2017 – (Isabelle Chrisment as reviewer)
- Xiao Han, Phd in Computer Science from TELECOM ParisTech, France. Title: Measurement and Monitoring of Security from the Perspective of a Service Provider, September 2017 – (Isabelle Chrisment as reviewer)
- Bruno Dorsemaine, Phd in Computer Science from TELECOM ParisTech, France. Title: Conception et expérimentation d'un modèle de sécurité dédié à un système d'information interagissant avec des infrastructures d'objets connectés, October 2017 – (Isabelle Chrisment as examiner)
- Rishikesh SAHAY, Phd in Computer Science from TELECOM ParisTech, France. Title: Policy-Driven Autonomic Cyberdefense using Software Defined Networking, November 2017 – (Isabelle Chrisment as examiner)
- Florian Grandhomme, Phd in Computer Science from Université de Rennes 1, France. Title: Études de protocoles de routage dynamique externe de type BGP dans un environnement réseaux tactiques ad hoc mobiles : faisabilité et performance, November 2017 – (Isabelle Chrisment as examiner)
- Celestin Matte, Phd in Computer Science from Université de Lyon, Insa, France. Title: Wi-Fi Tracking: Fingerprinting Attacks and Counter-Measures, December 2017 – (Isabelle Chrisment as examiner)
- Zied Aouini, Phd in Computer Science from Université de la Rochelle, France. Title: Traffic Monitoring in Home Networks: From Theory to Practice, December 2017 – (Isabelle Chrisment as reviewer)
- Deepak Subramanian, Phd in Computer Science from CentraleSupélec, France. Title: Information Flow Control for the Web Browser through a Mechanism of Split Qddress, December 2017 – (Isabelle Chrisment as reviewer)
- Emilie Bérard-Deroche, Phd in Computer Science from Université de Toulouse - INP Toulouse, France. Title: Distribution d'une architecture modulaire intégrée dans un contexte hélicoptère, December 2017 – (Yeqiong Song as reviewer)
- Alemayehu Addisu Desta, Phd in Computer Science from Université de Paris-Est, France. Title: Energy Supply and Demand Side Management in Industrial Microgrid Context, December 2017 – (Yeqiong Song as examinator)
- Muhammad Agus Zainuddin, Phd in Computer Science from Université de Franche-Comté, France. Title: Efficient Low Layer Techniques for Electromagnetic Nanocommunication Networks, March 2017 – (Yeqiong Song as reviewer)

Team members participated to the following mid-term Ph.D. defense committees in:

- Philippe Pittoli, PhD Student in Université de Strasbourg, France. Title : Architecture de sécurité pour l'Internet des Objets, July 2017 – (Isabelle Chrisment as external reviewer)
- Antoine Vastel, PhD Student in Université de Lille, France. Title; Browser Fingerprinting: Privacy, Security and tracking, September 2017 – (Isabelle Chrisment as external reviewer)
- John Harrison Kurunathan, PhD Student in the University of Porto, Portugal. Title: Improving QoS for IEEE 802.15.4e Networks, September 2017 – (Yeqiong Song as external reviewer)

Team members participated to the following Habilitation Degree defense committees:

- Mathieu Bouet, Habilitation Degree in Computer Science from Université Pierre et Marie Curie - Sorbonne Universités, France. Title: Software networks : Orchestration, resilience, and programmability concerns, July 2017 – (Olivier Festor as reviewer).
- Nader Mbarek, Habilitation Degree in Computer Science from Université de Bourgogne, France. Title: Contributions à la Gestion Autonome et la Garantie du Niveau de Service dans les Environnements Cloud, Radio Maillés et Mobiles, July 2017 – (Olivier Festor as reviewer).
- Osman Salem, Habilitation Degree in Computer Science from Université Paris Descartes, France. Title: Anomaly Detection in Wireless Body Area Networks for Reliable Healthcare Monitoring, April 2017 – (Olivier Festor as reviewer).
- Francis Colas, Habilitation Degree in Computer Science from Université de Lorraine, France. Title: Modélisation bayésienne et robotique, May 2017 – (Yeqiong Song as examinator).
- Hanen Idoudi, Habilitation Degree in Computer Science from Université Jean Jaures, Toulouse 2, France. Title: Contributions à l'amélioration des communications dans les réseaux sans fil multi-sauts, December 2017 – (Yeqiong Song as reviewer).
- Karine Deschinkel, Habilitation Degree in Computer Science from Université de Franche-Comté, France. Title: Nouveaux modèles de programmation linéaires et de flots pour la résolution de problèmes d'optimisation difficiles, June 2017 – (Yeqiong Song as president).

10.3. Popularization

- Isabelle Chrisment was in charge of the scientific part of the 4th module (connecter le réseau) in the Class'Code project https://project.inria.fr/classcode/classcode-in-english/, aiming at helping teachers and educators for introducing computer science to childrens aged from 8 to 14 years;

11. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] W. M. Shbair. *Service-Level Monitoring of HTTPS Traffic*, Université de Lorraine, May 2017, https://tel.archives-ouvertes.fr/tel-01649735

[2] J. Vaubourg. *Integration of IP network models to DEVS multi-models, for cyber-physical system co-simulations*, Université de Lorraine, April 2017, https://tel.archives-ouvertes.fr/tel-01647881

Articles in International Peer-Reviewed Journals

[3] F. De Turck, J.-M. Kang, H. Choo, M.-S. Kim, B.-Y. Choi, R. Badonnel, J. W.-K. Hong. *Softwarization of networks, clouds, and internet of things*, in "International Journal of Network Management", March 2017, vol. 27, n° 2, pp. 1-2 [*DOI :* 10.1002/nem.1967], https://hal.inria.fr/hal-01630838

[4] A. Mayzaud, R. Badonnel, I. Chrisment. *A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks*, in "IEEE Transactions on Network and Service Management", June 2017, vol. 14, n^{o} 2, pp. 472 - 486 [*DOI :* 10.1109/TNSM.2017.2705290], https://hal.inria.fr/hal-01630840

Invited Conferences

[5] L. Nussbaum. *Experimenting on Architectures for High Performance Computing*, in "École ARCHI 2017 - Architectures des Systèmes Matériels et Logiciels Embarqués et Méthodes de Conception Associées", Nancy, France, March 2017, 65 p. , https://hal.inria.fr/hal-01538680

[6] L. Nussbaum. *Scaling your experiments*, in "École RESCOM 2017", Le Croisic, France, June 2017, https://hal.inria.fr/hal-01577847

[7] L. Nussbaum. *Testbeds in Computer Science*, in "Reproducible Research Webinars", Grenoble, France, June 2017, https://hal.inria.fr/hal-01538683

International Conferences with Proceedings

[8] E. Aubry, T. Silverston, I. Chrisment. *Implementation and Evaluation of a Controller-Based Forwarding Scheme for NDN*, in "AINA 2017 - IEEE 31st International Conference on Advanced Information Networking and Applications", Taipei, Taiwan, IEEE, March 2017, pp. 144 - 151 [*DOI :* 10.1109/AINA.2017.83], https://hal.archives-ouvertes.fr/hal-01616234

[9] V. V. Avrutov, P. M. Aksonenko, P. Henaff, L. Ciarletta. *3D-Calibration of the IMU*, in "ELNANO 2017 - IEEE 37th International Conference on Electronics and Nanotechnology", KIEV, Ukraine, Electronics and Nanotechnology (ELNANO), 2017 IEEE 37th International Conference on, IEEE, April 2017, pp. 1-6 [*DOI :* 10.1109/ELNANO.2017.7939782], https://hal.archives-ouvertes.fr/hal-01654279

[10] A. Belkadi, H. Abaunza, L. Ciarletta, P. Castillo, D. Theilliol. *Distributed path planning for controlling a fleet of UAVs : application to a team of quadrotors*, in "20th IFAC World Congress, IFAC 2017", Toulouse, France, July 2017, https://hal.archives-ouvertes.fr/hal-01537777

[11] P. Chaignon, K. Lazri, J. Francois, O. Festor. *Understanding Disruptive Monitoring Capabilities of Programmable Networks*, in "NetSoft 2017 - IEEE Conference on Network Softwarization- NetFoG Workshop", Bologna, Italy, July 2017, https://hal.inria.fr/hal-01636117

[12] J. Charlier, S. Lagraa, R. State, J. Francois. *Profiling Smart Contracts Interactions with Tensor Decomposition and Graph Mining*, in "European Conference on Machine Learning and Principles and Practice of Knowledge Discovery (ECML-PKDD) - Workshop on MIning DAta for financial applicationS (MIDAS)", Skopje, Macedonia, September 2017, https://hal.inria.fr/hal-01636450

[13] M. Compastié, R. Badonnel, O. Festor, R. He, M. Kassi Lahlou. *Towards a Software-Defined Security Framework for Supporting Distributed Cloud*, in "AIMS 2017 - IFIP International Conference on Autonomous Infrastructure, Management and Security", Zurich, Switzerland, LNCS, Springer, July 2017, vol. 10356, pp. 47-61 [*DOI :* 10.1007/978-3-319-60774-0_4], https://hal.inria.fr/hal-01630852

[14] F. GREFF, Y.-Q. Song, L. Ciarletta, A. Samama. *A Dynamic Flow Allocation Method for the Design of a Software-Defined Real-Time Mesh Network*, in "WFCS 2017 - 13th IEEE International Workshop on Factory Communication Systems", Trondheim, Norway, Proceedings of the 13th IEEE International Workshop

on Factory Communication Systems (WFCS 2017), May 2017 [*DOI :* 10.1109/WFCS.2017.7991949], https://hal.inria.fr/hal-01529837

[15] F. GREFF, Y.-Q. SONG, L. CIARLETTA, A. SAMAMA. *Combining Source and Destination-Tag Routing to Handle Fault Tolerance in Software-Defined Real-Time Mesh Networks*, in "25th International Conference on Real-Time Networks and Systems", Grenoble, France, October 2017, https://hal.inria.fr/hal-01614268

[16] S. LAGRAA, J. FRANCOIS, A. LAHMADI, M. MINER, C. HAMMERSCHMIDT, R. STATE. *BotGM: Unsupervised Graph Mining to Detect Botnets in Traffic Flows*, in "CSNet 2017 - 1st Cyber Security in Networking Conference", Rio de Janeiro, Brazil, October 2017, https://hal.inria.fr/hal-01636480

[17] *Best Paper*
S. LAGRAA, J. FRANCOIS. *Knowledge Discovery of Port Scans from Darknet*, in "IFIP/IEEE Symposium on Integrated Network and Service Management (IM) - AnNet workshop", Lisbonne, Portugal, May 2017, https://hal.archives-ouvertes.fr/hal-01636215.

[18] D. I. MAXIM, R. DAVIS, L. I. CUCU-GROSJEAN, A. EASWARAN. *Probabilistic Analysis for Mixed Criticality Systems using Fixed Priority Preemptive Scheduling*, in "RTNS 2017 - International Conference on Real-Time Networks and Systems", Grenoble, France, October 2017, 10 p. [*DOI :* 10.1145/3139258.3139276], https://hal.inria.fr/hal-01614684

[19] D. MAXIM, Y.-Q. SONG. *Delay Analysis of AVB traffic in Time-Sensitive Networks (TSN)*, in "RTNS 2017 - International Conference on Real-Time Networks and Systems", Grenoble, France, October 2017, 10 p. [*DOI :* 10.1145/3139258.3139283], https://hal.inria.fr/hal-01614677

[20] L. MEFTAH, M. GOMEZ, R. ROUVOY, I. CHRISMENT. *AndroFleet: Testing WiFi Peer-to-Peer Mobile Apps in the Large*, in "ASE 2017 - 32nd IEEE/ACM International Conference on Automated Software Engineering", Urbana-Champaign, Illinois, United States, ASE 2017 - The 32nd IEEE/ACM International Conference on Automated Software Engineering - Tool demonstration, October 2017, https://hal.inria.fr/hal-01574466

[21] T. NGUYEN, X. MARCHAL, G. DOYEN, T. CHOLEZ, R. COGRANNE. *Content Poisoning in Named Data Networking: Comprehensive Characterization of real Deployment*, in "15th IFIP/IEEE International Symposium on Integrated Network Management (IM2017)", Lisbon, Portugal, May 2017, pp. 72-80 [*DOI :* 10.23919/INM.2017.7987266], https://hal.inria.fr/hal-01652328

[22] L. NUSSBAUM. *Testbeds Support for Reproducible Research*, in "ACM SIGCOMM 2017 Reproducibility Workshop", Los Angeles, United States, August 2017, https://hal.inria.fr/hal-01577849

[23] L. NUSSBAUM. *Towards Trustworthy Testbeds thanks to Throughout Testing*, in "REPPAR - 4th International Workshop on Reproducibility in Parallel Computing (with IPDPS'2017)", Orlando, United States, June 2017, 9 p. , https://hal.inria.fr/hal-01538682

[24] N. SCHNEPF, R. BADONNEL, A. LAHMADI, S. MERZ. *Automated Verification of Security Chains in Software-Defined Networks with Synaptic*, in "NetSoft 2017 - IEEE Conference on Network Softwarization", Bologna, Italy, IEEE Computer Society, July 2017, 9 p. [*DOI :* 10.1109/NETSOFT.2017.8004195], https://hal.inria.fr/hal-01630806

[25] S. SIGNORELLO, S. MARCHAL, J. FRANCOIS, O. FESTOR, R. STATE. *Advanced Interest Flooding Attacks in Named-Data Networking*, in "NCA 2017 - IEEE International Symposium on Network Computing and Applications", Cambridge, United States, October 2017, https://hal.inria.fr/hal-01636494

[26] S. ZHUO, Y. SONG. *GoMacH: A Traffic Adaptive Multi-channel MAC Protocol for IoT*, in "The 42nd IEEE Conference on Local Computer Networks (LCN)", Singapore, Singapore, October 2017, https://hal.inria.fr/hal-01616834

National Conferences with Proceedings

[27] S. DELAMARE, P. MORILLON, L. NUSSBAUM. *Réalisation d'expériences avec Grid'5000*, in "JRES2017 - Journées Réseaux de l'enseignement et de la recherche", Nantes, France, November 2017, https://hal.inria.fr/hal-01639524

Conferences without Proceedings

[28] M. ABDERRAHIM, M. OUZZIF, K. GUILLOUARD, J. FRANCOIS, A. LÈBRE. *A Holistic Monitoring Service for Fog/Edge Infrastructures: a Foresight Study*, in "The IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud 2017)", Prague, Czech Republic, August 2017, https://hal.archives-ouvertes.fr/hal-01591161

[29] V. AVRUTOV, P. AKSONENKO, N. BOURAOU, H. PATRICK, L. CIARLETTA. *Expanded Calibration of the MEMS Inertial Sensors*, in "UKRCON 2017 - IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON)", KIEV, Ukraine, May 2017 [*DOI :* 10.1109/UKRCON.2017.8100328], https://hal.archives-ouvertes.fr/hal-01654275

[30] S. BEN-AMOR, D. MAXIM, L. CUCU. *Schedulability analysis of dependent probabilistic real-time tasks* , in "MAPSP 2017 - 13th Workshop on Models and Algorithms for Planning and Scheduling Problems", Seeon-Seebruck, Germany, RTNS '16 Proceedings of the 24th International Conference on Real-Time Networks and Systems, ACM, June 2017, pp. 99-107 [*DOI :* 10.1145/2997465.2997499], https://hal.archives-ouvertes.fr/hal-01666138

[31] Z. LIU, L. CIARLETTA, C. YUAN, Y. ZHANG, D. THEILLIOL. *Path following control of unmanned quadrotor helicopter with obstacle avoidance capability*, in "International Conference on Unmanned Aircraft Systems, ICUAS'17", Miami, Florida, United States, June 2017, https://hal.archives-ouvertes.fr/hal-01537732

[32] D. MAXIM, A. BERTOUT. *Analysis and Simulation Tools for Probabilistic Real-Time Systems*, in "8th International Workshop on Analysis Tools and Methodologies for Embedded and Real-time Systems (WATERS)", Dubrovnik, Croatia, June 2017, https://hal.archives-ouvertes.fr/hal-01552798

[33] P. NEYRON, L. NUSSBAUM. *Resources management on the Grid'5000 testbed*, in "GEFI 17 meeting - Global Experimentation for Future Internet", Rio de Janeiro, Brazil, October 2017, https://hal.inria.fr/hal-01626320

[34] L. NUSSBAUM. *Testing Testbeds Towards Reproducibility*, in "GEFI 17 meeting - Global Experimentation for Future Internet", Rio de Janeiro, Brazil, October 2017, https://hal.inria.fr/hal-01626303

Scientific Books (or Scientific Book chapters)

[35] T. COMBE, W. MALLOULI, T. CHOLEZ, G. DOYEN, B. MATHIEU, E. MONTES DE OCA. *A SDN and NFV use-case: NDN implementation and security monitoring*, in "Guide to Security in SDN and NFV",

Computer Communications and Networks book series (CCN), Springer, November 2017, https://hal.inria.fr/hal-01652639

[36] D. MAXIM, L. CUCU-GROSJEAN, R. DAVIS. *Probabilistic schedulability analysis* , in "Handbook on Real-Time Computing", A. EASWARAN (editor), Handbook on Real-Time Computing, Springer, 2017, forthcoming, https://hal.archives-ouvertes.fr/hal-01666110

Books or Proceedings Editing

[37] R. BADONNEL, K. KINOSHITA, D. TUNCER, S. SONG (editors). *Special Issue on management of SDN/NFV-based systems*, Wiley, June 2017 [*DOI :* 10.1002/NEM.1982], https://hal.inria.fr/hal-01630991

[38] D. TUNCER, R. KOCH, R. BADONNEL, B. STILLER (editors). *Security of Networks and Services in an All-Connected World - 11th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security (IFIP AIMS 2017)*, July 2017, https://hal.inria.fr/hal-01630984

Other Publications

[39] F. GREFF, Y.-Q. SONG, A. SAMAMA, L. CIARLETTA. *Software-Defined Real-Time Mesh Networking: Protocol and Experimentation Method*, June 2017, RESCOM'17, Poster, https://hal.inria.fr/hal-01542911

[40] B. HENRY. *Approximations of the allelic frequency spectrum in general supercritical branching populations*, January 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01445838

[41] P. NEYRON, B. BZEZNIK, L. NUSSBAUM. *Propositions pour l'architecture pour un cluster mutualisé entre CIMENT et Grid'5000*, January 2017, working paper or preprint, https://hal.inria.fr/hal-01511285

[42] T. PARIS, L. CIARLETTA, V. CHEVRIER. *Intégration d'un simulateur multi-agent dans une plateforme de co-simulation DEVS*, July 2017, Journées Francophones sur les Systèmes Multi-Agents (JFSMA 2017), Poster, https://hal.archives-ouvertes.fr/hal-01567279

References in notes

[43] B. CAMUS, T. PARIS, J. VAUBOURG, Y. PRESSE, C. BOURJOT, L. CIARLETTA, V. CHEVRIER. *MECSYCO: a Multi-agent DEVS Wrapping Platform for the Co-simulation of Complex Systems*, LORIA, UMR 7503, Université de Lorraine, CNRS, Vandoeuvre-lès-Nancy ; Inria Nancy - Grand Est (Villers-lès-Nancy, France), September 2016, https://hal.inria.fr/hal-01399978

[44] H. PATRICK, V. AVRUTOV, P. AKSONENKO, N. BOURAOU, L. CIARLETTA. *Expanded Calibration of the MEMS Inertial Sensors*, in "Ukraine Conference on Electrical and Computer Engineering (UKRCON)", KIEV, Ukraine, May 2017, https://hal.archives-ouvertes.fr/hal-01654275

[45] 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