IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2016

Project-Team MADYNES

Management of dynamic networks and services

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

RESEARCH CENTER
Nancy - Grand Est

THEME
Networks and Telecommunications

Table of contents

1. Members **1**
2. Overall Objectives **3**
3. Research Program **4**
4. Highlights of the Year **4**
5. New Software and Platforms **4**
5.1. Distem 4
5.2. Grid'5000 testbed 5
5.3. Kadeploy 5
5.4. MECSYCO-RE-C++ 5
5.5. MECSYCO-RE-java 6
5.6. NDNperf 6
5.7. Ruby-cute 6
6. New Results **6**
6.1. Monitoring 6
6.1.1. Quality of Experience Monitoring 6
6.1.2. Active Monitoring 7
6.1.3. SDN enhanced monitoring 7
6.1.4. Service-level Monitoring of HTTPS traffic 7
6.1.5. Sensor networks monitoring 8
6.2. Security 9
6.2.1. Security analytics 9
6.2.2. DDoS Signaling 9
6.2.3. NDN Security 9
6.2.4. Configuration security automation 10
6.3. Experimentation, Emulation, Reproducible Research 11
6.3.1. Grid'5000 design and evolutions 11
6.3.2. Emulation with Distem 11
6.3.3. Management of experiments 11
6.3.4. Experimentation methodologies on Big Data 11
6.4. Routing 12
6.4.1. Probabilistic Energy-Aware Routing for Wireless Sensor Networks 12
6.4.2. NDN router with P4 12
6.4.3. NDN/HTTP cohabitation 12
6.5. Multi-modeling and co-simulation 13
6.6. Pervasive or Ubiquious Computing 14
6.7. Quality-of-Service 15
6.7.1. Self-adaptive MAC protocol for both QoS and energy efficiency 15
6.7.2. QoS and fault-tolerance in distributed real-time systems 15
6.7.3. Wireless sensor and actuator networks 15
6.7.4. NDN performance evaluation 16
7. Bilateral Contracts and Grants with Industry **16**
7.1. Bilateral Contracts with Industry 16
7.2. Bilateral Grants with Industry 16
8. Partnerships and Cooperations **17**
8.1. Regional Initiatives 17
8.1.1. 6PO Research Region Lorraine and UL project 17
8.1.2. Hydradrone FEDER Région Lorraine project 17
8.1.3. Satelor AME Lorraine regional project 18
8.2. National Initiatives 18

8.2.1. ANR BottleNet 18
8.2.2. ANR Doctor 19
8.2.3. PIA LAR 20
8.2.4. FUI HUMA 20
8.2.5. Inria-Orange Joint Lab 20
8.2.6. CNRS-INS2I PEPS NEFAE 21
8.2.7. CNRS-INS2I PEPS SURF 21
8.2.8. ANR FLIRT 21
8.2.9. Technological Development Action (ADT) 22
8.2.9.1. ADT UASS 22
8.2.9.2. ADT VERTEX 22
8.2.9.3. ADT COSETTE 22
8.2.9.4. ADT RIOT 22
8.2.10. Inria Project Lab 23
8.3. European Initiatives 23
8.3.1. FP7 & H2020 Projects 23
8.3.2. Collaborations in European Programs, Except FP7 & H2020 24
8.4. International Initiatives 24
8.4.1.1. IoT4D 24
8.4.1.2. Masdin 24
8.4.1.3. STIC-AmSud AKD Project 24
9. Dissemination **25**
9.1. Promoting Scientific Activities 25
9.1.1. Scientific Events Organisation 25
9.1.2. Scientific Events Selection 25
9.1.2.1. Chair of Conference Program Committees 25
9.1.2.2. Member of the Conference Program Committees 25
9.1.3. Journal 26
9.1.3.1. Member of the Editorial Boards 26
9.1.3.2. Reviewer - Reviewing Activities 26
9.1.4. Invited Talks 27
9.1.5. Scientific Expertise 27
9.2. Teaching - Supervision - Juries 27
9.2.1. Teaching 27
9.2.2. Supervision 28
9.2.2.1. PhD in progress in team 28
9.2.2.2. PhD defended in team 29
9.2.3. Juries 29
10. Bibliography **30**

Project-Team MADYNES

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

Keywords:

Computer Science and Digital Science:

1.1.4. - High performance computing
1.1.6. - Cloud
1.1.7. - Peer to peer
1.2. - Networks
1.3. - Distributed Systems
1.5. - Complex systems
4.1. - Threat analysis
4.9. - Security supervision
6.1.2. - Stochastic Modeling (SPDE, SDE)
6.1.3. - Discrete Modeling (multi-agent, people centered)
6.1.5. - Multiphysics modeling
6.2.6. - Optimization

Other Research Topics and Application Domains:

2.5.3. - Assistance for elderly
4.5. - Energy consumption
5.1. - Factory of the future
6.3.2. - Network protocols
6.3.3. - Network Management
6.4. - Internet of things
6.5. - Information systems
6.6. - Embedded systems
8.1. - Smart building/home
8.5. - Smart society
9.5.10. - Digital humanities
9.6. - Reproducibility

1. Members

Research Scientists

Jérôme François [Inria, Researcher]
Vassili Rivron [Inria, Researcher]

Faculty Members

Isabelle Chrisment [Team leader, Univ. Lorraine, Professor, HDR]
Laurent Andrey [Univ. Lorraine, Associate Professor]
Rémi Badonnel [Univ. Lorraine, Associate Professor]
Thibault Cholez [Univ. Lorraine, Associate Professor]
Laurent Ciarletta [Univ. Lorraine, Associate Professor]
Olivier Festor [Univ. Lorraine, Professor, HDR]

Abdelkader Lahmadi [Univ. Lorraine, Associate Professor]
Emmanuel Nataf [Univ. Lorraine, Associate Professor]
Lucas Nussbaum [Univ. Lorraine, Associate Professor]
Thomas Silverston [Univ. Lorraine, Associate Professor]
Yeqiong Song [Univ. Lorraine, Professor, HDR]

Engineers

Raphael Cherfan [Inria, until Aug 2016]
François Despaux [Univ. Lorraine]
Florent Didier [Inria, from Nov 2016]
Cédric Enclos [Univ. Lorraine, until Jun 2016]
Jérémie Gaidamour [Inria, until Sep 2016]
Adrien Guenard [Univ. Lorraine]
Sofiane Lagraa [Inria]
Clement Parisot [Inria]
Yannick Presse [Inria, granted by EDF]
Loic Rouch [Inria]
Cristian Camilo Ruiz Sanabria [Inria, until Oct 2016]
Benjamin Segault [Univ. Lorraine , until Oct 2016]
Alexandre Tan [Inria, granted by EDF]
Shuguo Zhuo [Inria]

PhD Students

Petro Aksonenko [Univ. Lorraine, from Jun 2016]
Jonathan Arnault [Inria, until Jun 2016]
Elian Aubry [Univ. Lorraine]
Pierre-Olivier Brissaud [Thales, granted by CIFRE]
Tomasz Buchert [Univ. Lorraine, until Jan 2016]
Paul Chaignon [Orange Labs, granted by CIFRE]
Maxime Compastie [Orange Labs, granted by CIFRE]
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]
Xavier Marchal [CNRS]
Anthea Mayzaud [Inria, until Oct 2016, granted by FP7 GA Flamingo project]
Thomas Paris [Univ. Lorraine]
Abdulqawi Saif [Xilopix, granted by CIFRE]
Nicolas Schnepf [Inria]
Wazen Shbair [Univ. Lorraine]
Salvatore Signorello [University of Luxembourg - Univ. Lorraine (co-advising)]
Evangelia Tsiontsiou [Univ. Lorraine]
Julien Vaubourg [Univ. Lorraine]
Kévin Roussel [Inria, until Sep 2016]

Post-Doctoral Fellows

Benoit Henry [Univ. Lorraine, until Nov 2016]
Mohamed Tlig [Univ. Lorraine, until Jun 2016]
Zhixiang Liu [Univ. Lorraine, from Dec 2016]
Lei Mo [Univ. Lorraine, until Sep 2016]

Visiting Scientist

Hong Zhou [Univ. Lorraine, from Sep 2016 until Oct 2016]

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

Others
Paul Andrey [Univ. Lorraine, Internship ENSAE, from Jul 2016 until Aug 2016]
Nicolas Bedrine [Inria, Internship TELECOM Nancy, from Jun 2016 until Jul 2016]
Sébastien Coorevits [Inria, Internship TELECOM Nancy, from Jun 2016 until Jul 2016]
Marc Coudriau [Inria, Internship ENS Paris, from Jun 2016 until Aug 2016]
Yassine Elmrabet [Univ. Lorraine, Internship, from Mar 2016 until Jul 2016]
Mohamed Ezzeddine [Inria, Internship TELECOM Nancy, from Jun 2016 until Aug 2016]
Arthur Garnier [Inria, élève ingénieur en apprentissage, TELECOM Nancy]
Adrien Pheulpin [Inria, Internship TELECOM Nancy, from Jun 2016 until Aug 2016]
Antoine Richard [Univ. Lorraine, Internship from Sept 2016 until Dec 2016]
Quentin Rouy [Univ. Lorraine, Internship TELECOM Nancy, from Jun 2016 until Jul 2016]
Valentin Stern [Univ. Lorraine, Internship TELECOM Nancy, until Jul 2016]
Yoann Switala [Inria, Internship TELECOM Nancy, from Jun 2016 until Jul 2016]

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. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Masdin associate team

Thanks to previously existing collaborations, a new associate team with SnT at University of Luxembourg has been created in 2016 with a focus on softwarization of networks.

5. New Software and Platforms

5.1. 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 - Grid'5000 - Inria - Loria - Université de Lorraine
- Contact: Lucas Nussbaum
- URL: http://distem.gforge.inria.fr

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

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

5.4. MECSYCO-RE-C++

Multi-agent Environment for Complex SYstems COsimulation. Cœur C++
KEYWORDS: Modeling - Simulation - Simulator - Multi-model - Multi-agent - Agent - 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 vizualizing simulations).

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

5.5. MECSYCO-RE-java

Multi-agent Environment for Complex SYstems COsimulation. Coeur java
KEYWORDS: Modeling - Simulation - Simulator - Multi-model - Co-simulation - Multi-agent - Agent - 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 complimente by mecsyco-com (a communication package for distributed exécution) and mecsyco-visu (a set of tools for vizualizing simulations).

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

5.6. NDNperf

KEYWORDS: Performance measure - Named-Data Networking
FUNCTIONAL DESCRIPTION

We designed NDNperf, an open source tool for NDN server-side performance evaluation and sizing purposes, in order to have an idea of the throughput a server can achieve when it has to generate and transmit NDN Data packets. It is very similar to iPerf and also needs a client and a server to perform the measurements while minimizing the number of instructions between Interest reception and Data emission. It has the following features: - Periodic report of performances: end-to-end throughput, latency, processing time, - Fresh NDN Data generation or NDN Data delivery from caches, - Multi-threaded (one main thread for event lookup and N threads for NDN Data generation), - Able to use all available signatures implemented in the NDN library, choose the size of the key, and the transmission size of Data packets.

- Contact: Thibault Cholez
- URL: http://madynes.loria.fr/software/

5.7. 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. New Results

6.1. Monitoring

6.1.1. Quality of Experience Monitoring

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

We have pursued our work on smartphone usage monitoring. In [26], we presented an exploratory smartphone usage study with logs collected from users in the wild, combined with the sociodemographic, technological and cultural information provided by them. We have shown that application usage among users is highly diverse. However when the applications are grouped as services, interesting relations appear between user profiles and types of services used. We found significant correlations between service usage and socio-demographic profile. We have proposed several possible use cases of how sociological information can be used to renew the official statistics, to recommend suitable applications to potential users.

6.1.2. Active Monitoring

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

Following preliminary work in 2015, we pursued our assessment of industrial system exposition in the Internet. Industrial systems are composed of multiple components whose security has not been addressed for a while. Even if recent propositions target to improve it, they are still often exposed to vulnerabilities, since their components are hard to update or replace. In parallel, they tend to be more and more exposed in the public Internet for convenience. Although awareness of such a problem has been raised, there is no precise evaluation of such a risk. We thus defined a methodology to measure the exposure of industrial systems through Internet. In particular, a carefully designed scanning approach and software with a low footprint, named WiScan, consists in optimizing the distance between consecutively scanned IP addresses but being fast to compute. It has been applied on the entire IPv4 address space, by targeting specific SCADA ports. This work is reported in [20].

During the year 2016, we are also working with the regional PME TracIP http://www.tracip.fr on the development of attack assessment and forensics platform dedicated to industrial control system. The platform involves multiple PLC from different manufactures and real devices of factory automation systems.

6.1.3. SDN enhanced monitoring

Participants: Jérôme François [contact], Lautaro Dolberg [University of Luxembourg].

Software-Defined Networking (SDN) provides a highly flexible flow management platform through a logically centralized controller that exposes network capabilities to the applications. However, most applications do not natively use SDN. An external entity is thus responsible for defining the corresponding flow management policies. This is mainly the role of the network administrator, which also prefers to keep the control of its network rather than fully let the control to users or applications.

Usually network operators prefer to control the flow management policies, rather than granting full control to the applications. Although IP addresses and port numbers can suffice to identify users and applications in ISP networks and determine the policies applicable to their flows, such an assumption does not hold strongly in cloud environments. IP addresses are allocated dynamically to the users, while port numbers can be freely chosen by users or cloud-based applications. These applications, like computing or storage frameworks, use diverse port numbers which amplifies this phenomenon. We have proposed higher-level abstractions for defining user- and application-specific policies. In this scope, our framework transparently maps application-level policies (involving application and user names) to OpenFlow rules (IP addresses, protocols and port numbers), which alleviates the necessity for the control applications (those interacting with the Northbound interface of the controller) to keep track of the network characteristics (like location) of users and applications themselves. To achieve this end, application-level information is retrieved in real-time through local remote system agents, which can be easily deployed in a cloud platform where both network and computational infrastructure are hosted by the same entity.

Thus our work enables the association of flows with applications and users. It led to a publication [19].

6.1.4. Service-level Monitoring of HTTPS traffic

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

We previously investigated the latest technique for HTTPS traffic filtering that is based on the Server Name Indication (SNI) field of TLS and which has been recently implemented in many firewall solutions. We showed that SNI has two weaknesses, regarding (1) backward compatibility and (2) multiple services using a single certificate. On the other side, HTTPS proxy suffers from privacy issues by decrypting users' sensitive traffic. This led us to the development of new reliable methods to investigate the increasing number of HTTPS traffic with a proper level of identification (service-level) that allows the management of the traffic while other methods are either too broad (protocol-lvl identification) or too precise (page-level identification).

We proposed to improve HTTPS traffic monitoring based on SNI. Our investigation shows that 92% of the HTTPS websites surveyed can be accessed with fake-SNI. Our approach verifies the coherence between the real destination server and the claimed value of SNI by relying on a trusted DNS service. Experimental results show the ability to overcome the shortage of SNI-based monitoring by detecting forged SNI values while having a very small false positive rate (1.7%). The overhead of our solution only adds negligible delays to access HTTPS websites. The proposed method opens the door to improve global HTTPS monitoring and firewall systems and was published in the IEEE STAM workshop [31].

We 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. This work was published in IFIP/IEEE NOMS [30] and is now extended in the frame of the CNRS PEPS NEFAE project to address the challenge of real-time monitoring of HTTPS. We extract statistical features on TLS handshake packets and progressively on application data packets, so that we can identify HTTPS services very early in the session. Extensive experiments performed over a significant and open dataset show that our method offers a good accuracy and a prototype implementation confirms that the real-time requirement of monitoring HTTPS services is satisfied.

6.1.5. Sensor networks monitoring

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

This year, we have pursued our work on IoT security monitoring, based on our distributed architecture specified in [24]. This one exploits the multi-instance mechanisms of the RPL protocol, to build a monitoring plane using high-order nodes, in the context of Advanced Metering Infrastructures (AMI). It permits to preserve more constrained node resources, by passively monitoring the network. We have shown in [23] its benefits for detecting version number attacks. A DODAG versioning system is incorporated into the RPL protocol, in order to ensure an optimized topology. However, an attacker can exploit this mechanism to damage the network and reduce its lifetime. We have therefore proposed a detection strategy with a set of algorithms capable of identifying malicious nodes performing such attacks. We have evaluated our solution through experiments and have analyzed the performance according to defined metrics. We have shown that false positive rates can be reduced by a strategic monitoring node placement. In particular, we have addressed scalability considerations, as an optimization problem which can be easily adapted to different topologies. By resolving this problem, we were able to quantify the number of monitoring nodes required to ensure an acceptable false positive rate for different topologies.

Our taxonomy on security attacks in these networks has also been published in [2]. The RPL protocol is exposed to a large variety of attacks, whose consequences can be quite significant in terms of network performance and resources. The attacks against resources reduce network lifetime through the generation of fake control messages or the building of loops. The attacks against the topology make the network converge to a sub-optimal configuration or isolated nodes. Attacks against network traffic let a malicious node capture and analyse large part of the traffic. This classification serves as a support to prioritize attacks depending on the damages they may cause to the network, and can be exploited for risk management purposes in order to select counter-measures.

6.2. Security

6.2.1. Security analytics

Participants: Jérôme François [contact], Abdelkader Lahmadi, Giulia de Santis, Marc Coudriau, Olivier Festor.

During 2016, active collaboration with the High Security Lab in Nancy continues especially in the context of the FUI HuMa project. First we developed a method to automatically analyze darknet data. A darknet or telescope is a whole subnetwork, which is announced over Internet such that packets sent to the IP addresses are properly routed over but not replied to. In our case, the darknet is a /20 network meaning that we monitor 2^{12} addresses. The main challenge we faced was to cope with the volume of data in order to extract intertwined phenomena characterized by groups of packets. We proposed a clustering and visualisation method derived from the Mapper algorithm that has been developed in the field of Topological Data Analysis (TDA). The developed method and its associated tool are able to analyze a large number of IP packets in order to make malicious activity patterns easily observable by security analysts. The results show that our method is able to exhibit observable patterns which have been missed by Suricata, a widely used State-of-the-Art IDS https://hal.inria.fr/hal-01403950/document.

Second scannings have been particularly studied as they represent the first phase of recognition in advanced persistent threats. While it is known that every exposed systems is always being actively scanned from multiple sources, it is still challenging to fingerprint them, in particular to identify what are the distributed sources of a single synchronized scan and what is the tool used to generate it. As a first step, we proposed a methodology based on Hidden Markov Models (HMMs) to model scanning activities monitored by a darknet [18]. The HMMs of scanning activities are built on the basis of the number of scanned IP addresses within a time window and fitted using mixtures of Poisson distributions.

We are also still maintaining an IRTF draft [50] to promote a standardization effort towards the extension of IP Flow-based monitoring with geographic information. Associating Flow information with their measurement points geographic locations will enable security applications to detect anomalous activities. In the case of mobile devices, the characterization of communication patterns using only time and volume is not enough to detect unusual location-related communication patterns. The draft went through an IRSG review and a feedback is still required from the OPSWAG IETF working group.

6.2.2. DDoS Signaling

Participants: Jérôme François [contact], Abdelkader Lahmadi, Giovane Moura [SIDN Labs, Netherland], Marco Davids [SIDN Labs, Netherlands].

A distributed denial-of-service (DDoS) attack aims at rendering machines or network resources unavailable. These attacks have grown in frequency, intensity and target diversity. In the context of Flamingo, Madynes contributed to the definition of an opportunistic signaling protocol in cooperation with SIDN Labs in Netherlands. The goal is to provide an efficient mechanism where nodes in an IPv6 network facing a DDoS attack can deliver a DOTS (DDoS Open Threat Signaling) signal message sent by a DOTS client to the DOTS server. The specified mechanism does not generate transport packets to carry the DOTS signal message but it only relies on existing IPv6 packets in the network to include within them a hop-by-hop extension header which contains an encoded DOTS signal message.

This work is done under the umbrella of our standardization activities especially within the IETF DOTS working group [45] and was presented during IETF 96 in Berlin.

6.2.3. NDN Security

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

Named-Data Networking (NDN) is one of the most advanced ICN architecture but the security of NDN or NFD (NDN Forwarding Deamin) is still in the early stages and not ready for real deployment. In the context of the ANR Doctor project, we investigate NDN security in order to unveil issues and propose remediations.

First, we discovered a new vulnerability of NDN which is easy to exploit and can lead to very serious attacks, badly affecting the network. This vulnerability is due to an absence of control at the precise moment when NFD receives an incoming Data. In fact, NFD only checks two points: if the Data belongs to the localhost scope, or if it matches an existing PIT entry, but not if the Data comes from a valid Face. This is a critical shortage because it allows malicious users to directly send Data to perform attacks like DoS and cache poisoning without having to register a prefix in the router's FIB beforehand to receive legitimate Interests. After these checks, NFD continues to process the Data packet. The NDN protocol makes the hypothesis that a node cannot send a Data packet without having previously received the corresponding Interest (receiver driven communication). However, NFD should consider malicious nodes that decide to not follow the standard way to proceed with NDN communications and send Data unexpectedly. We further described two serious attack scenarios exploiting this vulnerability based on the fact that malicious nodes can send unexpected Data that can consume legitimate PIT entries. We also propose two ways to prevent it with minor modifications in NFD. This work was published and demonstrated at the ACM-ICN conference [46].

Second, we addressed the Content Poisoning Attack (CPA), known to be one of the major threats in NDN. 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 the context of the ANR Doctor Project, and in collaboration with UTT, we demonstrated through an experimental measurement campaign that CPA can easily and widely affect NDN. We proposed three realistic attack scenarios relying on both protocol design and implementation weaknesses and presented their implementation and evaluation in a testbed based on the latest NFD version. We analyzed their impact on the different ICN nodes composing a realistic topology (clients, access and core routers, content provider) in order to fully characterize the CPA. This work has been accepted and will be published in IFIP/IEEE IM 2017 conference.

6.2.4. Configuration security automation

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

We have pursued during year 2016 our efforts on the orchestration of security functions in the context of mobile smart environments, with a joint work with Stephan Merz of the VeriDis project-team at Inria Nancy. In particular, Nicolas Schnepf studied during his Master thesis formal techniques for the automatic verification of chains of security functions in a setting of software-defined networks (SDN). Concretely, he defined an extension of the Pyretic language [51] which takes into account the data plane of SDN controllers and implemented a translation of that extension to the input languages of the nuXmv model checker and of SMT solvers. The approach and its scalability were validated over crafted security chains, and a conference paper describing the results is going to be submitted shortly. Nicolas Schnepf started a PhD thesis on the same topic in October 2016 with joint supervision by members of the Madynes and VeriDis Inria project-teams.

In addition, we have analyzed and evaluated the usage of OpenFlow messages for security applications [29], jointly with Bundeswehr University of Munich. The purpose was to quantify the performances of security solutions that are built on top of software-defined networking infrastructures. We have considered overloading attacks and information gathering attacks, that are quite common in these environments, and have detailed regular and sdn-based mitigation mechanisms that have been designed for tackling them. We have then analyzed for each category the dependencies of these mechanisms to the OpenFlow protocol commonly supporting the communications between sdn controllers and switches. These dependencies have been identified through the mapping of OpenFlow messages to security functionalities in that context. Based on this analysis, we performed series of experiments on two different testbeds for comparing and evaluating the accuracy and reliability that can be expected with respect to these messages.

We have also investigated in [16] a software- defined security framework, for supporting the enforcement of security policies in distributed cloud environments. These latter require security mechanisms able to address their multi-tenancy and multi-cloud properties. 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. It exploits a

security orchestrator, policy decision points (PDP) and policy enforcement point (PEP) interacting according to a dedicated set of protocols, and will take advantage of facilities offered by unikernel and micro-services techniques to reduce the security exposure of cloud resources. The proposed framework has been evaluated so far through a set of validation scenarios corresponding to a realistic use cases including cloud resource allocation/deallocation, cloud resource state change, and dynamic access control.

6.3. Experimentation, Emulation, Reproducible Research

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

6.3.1. Grid'5000 design and evolutions

Participants: Jérémie Gaidamour, Arthur Garnier, Lucas Nussbaum [contact], Clément Parisot, Florent Didier.

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

First, we finished the installation and setup of several new clusters in the Nancy site, which brought several new local users, from various teams, to the testbed.

In the context of ADT LAPLACE, Jérémie Gaidamour added support for the control of CPU parameters such as Hyperthreading, Turboboost, P-states and C-states. It is expected that this work will enable interesting usages in the areas of HPC runtimes and energy-aware computing.

Finally, in the context of his roles in the *bureau*, *comité d'architectes* and *comité des responsables de sites* of Grid'5000, Lucas Nussbaum managed the purchase of the new clusters at Nancy mentioned above, and gave several presentations about the testbed, at the *Grid'5000 School* [5] [38], at a GENI-FIRE collaboration workshop [9], [8], [6], [7].

6.3.2. Emulation with Distem

Participants: Emmanuel Jeanvoine, Lucas Nussbaum [contact], Cristian Ruiz.

Several improvements have been made around Distem, mostly in the context of ADT COSETTE.

A paper demonstrating the use of Distem to evaluate fault tolerance and load balancing strategies implemented in Charm++ was accepted at CCGrid'2016 [28].

We continued our work on using Distem to experiment on NDN infrastructures. We obtained promising results, especially in terms of scale. This work is still pending publication.

Finally, we also evaluated the porting of Distem to other testbeds (ChameleonCloud and CloudLab), which was interesting for Distem specifically, but also to understand differences between those testbeds [43].

6.3.3. Management of experiments

Participants: Tomasz Buchert, Emmanuel Jeanvoine, Lucas Nussbaum [contact], Cristian Ruiz.

We continued work on Ruby-Cute, a library that aggregates various useful functionality in the context of such tools. Several releases were made in 2016. We hope that it will be useful as a basis for future tools, and ease testing of new ideas in that field. The library is available on http://ruby-cute.github.io/.

Tomasz Buchert defended his PhD thesis, entitled *Managing large-scale, distributed systems research experiments with control-flows*, in January 2016 [1].

6.3.4. Experimentation methodologies on Big Data

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

Abdulqawi Saif started his PhD on experimentation methodologies for Big Data at the end of 2015. His first work [35] is a multi-criteria analysis of NFS performance using statistical Design of Experiments techniques.

6.4. Routing

6.4.1. Probabilistic Energy-Aware Routing for Wireless Sensor Networks

Participants: Evangelia Tsiontsiou, Bernardetta Addis, Alberto Ceselli [Universita degli Studi di Milano], Ye-Qiong Song [contact].

Healthcare applications are considered as promising fields for Wireless Sensor Networks (WSNs) and globally IoT. Thanks to WSNs, patients can be monitored in hospitals or smart home environments, providing health improvement, or emergency care. Network lifetime is still the key issue when we deploy wireless sensor networks and IoT solutions in real-world applications. Current WSN research trends include duty-cycling at MAC layer and energy efficient routing at network layer, among others. We proposed an Optimal Probabilistic Energy-Aware Routing Protocol (OPEAR) for duty-cycled WSNs which aims at maximizing the network lifetime by keeping low energy consumption and balancing network traffic between nodes. Our experimental campaign reveals that our OPEAR protocol outperforms the popular Energy Aware Routing Protocol (EAR) from the literature, proving to be more effective in extending the network lifetime [33]. It is part of Lorraine AME Satelor project granted by Lorraine Region.

6.4.2. NDN router with P4

Participants: Salvatore Signorello [University of Luxembourg], Olivier Festor [contact], Radu State [University of Luxembourg], Jérôme François.

Although content-awareness at the network level is becoming more and more needed, Information-Centric Networking (ICN)-based solutions struggle to emerge. Research on ICN has already produced insightful outputs, nevertheless architecture-tied designs of ICN devices cannot be easily deployed and tested in operational networks; further those designs are hard to share. In the meantime, the vision of Software-Defined Networking has grown and taken new shapes. Network players desire to change devices' behavior often and drastically, even though performances are still crucial to operate at line-speed. This has been leading to a rethink of network devices designs with the aim to offer full-programmability through high-level programming languages for packet processors, like P4. It is a programming language to describe the forwarding plane of network devices. The language abstracts how packets are processed by different devices in target- independent programs. Then, compilers map those programs to different forwarding devices with as final goal a single specification which can be automatically mapped to hardware or software implementations. Although high-level protocols like ICN with advanced parsing mechanisms are usually handled by software switch with standard programming capacity, P4 would allow more efficient implementation on specific platform. Our preliminary implementation strives to implement many features of the NDN routing by using native P4 language constructs only [32].

6.4.3. NDN/HTTP cohabitation

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

Network operators are reluctant to deploy globally Named Data Networking (NDN) because of the huge investment costs required and the uncertainty about the security and the manageability of such disruptive network protocols when deployed in production, while the return of investment is also uncertain. Meanwhile, Network Functions Virtualization (NFV) greatly facilitates the deployment of novel networking architectures by reducing the costs thanks to the usage of commodity hardware in place of dedicated equipments. Consequently, leveraging NFV to ease the deployment of NDN infrastructures appears as a strong mean to incite network operators to adopt this technology. In this context, the challenge we address in the ANR DOCTOR project is to fulfil the requirements needed to move NDN from a solution restricted to labs or tesbeds to a fully operational one by developing NDN-specific Virtual Network Functions (VNF).

In this effort, one of the main first questions which arise is about the integration of NDN into the existing Internet, and particularly the collocation of NDN with IP and HTTP. We think that a good way to deploy NDN consists in creating virtualized NDN island that can be crossed by specific content-related traffic, such as HTTP, and thus benefit from NDN properties (caching, aggregation, etc.). We proposed and developed an early version of a fully-capable NDN/HTTP gateway that can seamlessly connect a NDN network to the rest of the World Wide Web. This work was published and demonstrated at the ACM-ICN conference [47].

6.5. Multi-modeling and co-simulation

Participants: Laurent Ciarletta [contact], Olivier Festor, Ye-Qiong Song, Yannick Presse, Julien Vaubourg, Alexandre Tan, Benjamin Segault, Thomas Paris.

Vincent Chevrier (former Maia team, Dep 5, LORIA) is a collaborator and the correspondant for the MS4SG/MECSYCO project, Benjamin Camus, and Christine Bourjot (former MAIA team, Dep 5, LORIA) are collaborators for AA4MM/MECSYCO. Julien Vaubourg and Thomas Paris's PhDs are under the co-direction of V. Chevrier and L. Ciarletta.

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

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

We proposed the AA4MM meta-model [52] 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) projet 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.

In 2016 we worked on the following research topics:

- Assessment and evaluation of complex systems.
- Cyber Physical Systems.

  We have pursued the design and implementation of the Aetournos platform at Loria. The collective movements of a flock of flying communicating robots / UAVs, evolving in potentially perturbed environment constitute a good example of a Cyber Physical System.

  We have maintained thanks to the ADT UASS a set of tools: multi-simulation behavior / network / physics and generic software development using ROS (Robot Operating System). The UAVs carry a set of sensors for location awareness, their own computing capabilities and several wireless networks.
- MS4SG / MECSYCO-NG opportunity to link simulations tools with a strong focus on FMI (Functional Mockup Interface) and network simulators (NS3/Omnet++) thanks to our MECSYCO (formerly AA4MM) framework. We have so far successfully applied our solution to the simulation of smart apartment complex and to combine the electrical and networking part of a Smart Grid. The AA4MM software is now MECSYCO and has seen major improvements in 2016 thanks to the ressources provided by the MECSYCO-NG project in collaboration with EDF R&D (http://www.mecsyco.com).

  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.

  We have developed software components and plugins that interconnects within MECSYCO heterogeneous simulators from different domains: FMU (working with the 1.0 and 2.0 FMI standard for CoSimulation) ou non-FMU such as NS3 or Omnet++.

Several EDF oriented advanced use cases have demonstrated multi-simulations.

In addition to technical reports [41], several publications have been accepted in 2016 on these subjects [25], [13] and [34].

6.6. Pervasive or Ubiquious Computing

Participants: Laurent Ciarletta [contact], Olivier Festor, Ye-Qiong Song, Emmanuel Nataf, Thomas Paris, Benjamin Segault, Antoine Richard, Petro Aksonenko.

P. Aksonenko PhD is under the co-direction of L. Ciarletta and Patrick Henaff from Loria Dep 5. Thomas Gurriet, now PhD student at Georgia Tech under the supervision of Prs Eric Feron and Aaron Ames is contributing to the topic of CPS safety.

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, increasingly numerous and heterogeneous, are embedded in the fabric of our daily lives. Our initial subject of interest is to study them with regards to their complexity: Those 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 their surroundings and the environment. Secondly, the potential multiplicity and heterogeneity of devices, services, communication protocols, and the constant mobility and reorganization also need to be addressed. Thirdly we are aking into account their dynamcity, with regards to their mobility and evolving context.

Our research on this field is going towards both closing the loop between humans and systems, physical and computing systems, and taming the complexity, using multi-modeling (to combine the best of each domain specific model) and co-simulation (to design, develop and evaluate) as part of a global conceptual and practical toolbox.

In 2016 we mainly worked on the Cyber Physical Systems.

We maintained the Aetournos platform at Loria in collaboration with 6PO and the support of ADT UASS. We are studying the collective movements of a flock of flying communicating robots / UAVs, evolving in potentially perturbed environment constitute a good example of a Cyber Physical System.

The effort put in the UAVs gathers academic and research ressources from the Aetournos platform, the Inria ADT R2D2 and the 6PO project, while applied, industrial and more R&D projects have been pursued this year (Medical Express / Outback Joe Search and Rescue Challenge, Alerion, Hydradrone, and a CIFRE PhD with Thales for example) .

This also led to two new accepted projects:

- one Interreg “Grone”, a generic project about drones in industrial and agricultural environments, started in October 2016
- and one FUI22 “CEOS”, about insuring safety in UAVs at the system level that will start in 2017

  One of the emerging topic in this area is the safety of Mobile IoT / CPS with regards to their environment and users. This gave first results on how to design the internal communication system [21], the overal system [15], specific safety solutions [14] and a US Patent has been filled on a termination system led by Georgia Tech [Optimal Emergency Termination System for Unmanned Aerial Vehicles by Destructive Rotor Surface Reduction, Application No.: 62/378,923].
- Smart * (MECSYCO)

  We have studied scientific problems around models and simulators composition. We have also looked into practical and implementation issues in the frame of our MECSYCO /AA4MM solutions. We have added to our Smart Grid scenarios a smart appartment complex use case.
- (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.

6.7. Quality-of-Service

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

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

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

We have mainly contributed to enhancing the implementation of the high efficient traffic self-adaptive MAC protocols. As part of RIOT ADT project, we have improved and implemented a fully functional iQueue-MAC which provides not only the unique feature of high traffic self-adaptivity, but also the robustness by using two control channels (https://github.com/RIOT-OS/RIOT/pull/5618).

As part of LAR project, we were interested by using the Cooja/MSPSim network simulation framework for RIOT OS based platforms. We have showed that Cooja is not limited only to the simulation of the Contiki OS based systems and networks, but can also be extended to perform simulation experiments of other OS based platforms, especially that with RIOT OS. Moreover, when performing our own simulations with Cooja and MSPSim, we observed timing inconsistencies with identical experimentations made on actual hardware. Such inaccuracies clearly impair the use of the Cooja/MSPSim framework as a performance evaluation tool, at least for time-related performance parameters. The detailed results of our investigations on the inaccuracy problems, as well as the consequences of this issue, and possible ways to fix or avoid it are available in [27].

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

Participants: Florian Greff, Laurent Ciarletta, Arnauld Samama [Thales TRT], Eric Dujardin [Thales TRT], 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 started a study on the real-time dependability of distributed multi-criticity systems interconnected by an embedded mesh network (RapidIO). For easing the QoS specification at the higher level, DDS middleware is used. We postulate that enhancing QoS for real-time applications entails the development of a cross-layer support of high-level requirements, thus requiring a deep knowledge of the underlying networks. This year, we proposed and implemented a new simulation/emulation/experimentation framework called ERICA, for designing such a feature. ERICA integrates both a network simulator (Ptolemy) and an actual hardware network to allow implementation and evaluation of different QoS-guaranteeing mechanisms. It also supports real-software-in-the-loop, i.e. running of real applications and middleware over these networks [21].

We have also dealt with mesh networking of embedded components. Our approach is to allow applications to make online real-time flow resource requests and consequently dynamically allot network resources according to these requirements. To this end, additional mechanisms must be provided in order to meet the real-time constraints while the platform remains as dynamic as possible. We gather these mechanisms into a Software-Defined Real-time Network (SDRN) paradigm. The online admission control and pathfinding algorithms have been developed allowing the controller to dynamically configure the real-time network nodes. We have evaluated several pathfinding algorithms.

6.7.3. Wireless sensor and actuator networks

Participants: Lei Mo, Adrian Guenard, Yifei Qi [Zhejiang University], Jiming Chen [Zhejiang University], Ye-Qiong Song [contact].

Wireless sensor and actuator networks provide a key technology for fully interacting within a CPS (Cyber-Physical System). However, the introduction of the mobile actuator nodes in a network rises some new challenging issues. In this context, we addressed two important issues: the multiple target tracking using both fixed and mobile sensors and the optimal scheduling of mobile wireless energy chargers (actuators) for fixed sensor nodes.

In the low-cost and large-scale deployment of mobile sensor nodes for target tracking, due to the constraints of limited sensing range, it is of great importance to design node coordination mechanism for reliable tracking so that at least the target can always be detected with a high probability, while the total network energy cost can be reduced for longer network lifetime. In [3], we dealt with this problem considering both the unreliable wireless channel and the network energy constraint. We transfer the original problem into a dynamic coverage problem and decompose it into two subproblems. By exploiting the online estimate of target location, we first decide the locations where the mobile nodes should move into so that the reliable tracking can be guaranteed. Then, we assign different mobile nodes to each location in order that the total energy cost in terms of moving distance can be minimized. Extensive simulations under various system settings have shown the effectiveness of our solution.

We also investigated the multiple mobile chargers coordination problem that is minimizing the energy expenditure of the mobile chargers while guaranteeing the perpetual operation of the wireless sensor network. We extended our previous result (published in IPCCC2015) by taking into account mobile charger's charging ability. We formulated this problem as a mixed-integer linear program (MILP), and proposed a novel decentralized method which is based on Benders decomposition. The convergence of proposed method is analyzed theoretically. Simulation results demonstrate the effectiveness and scalability of the proposed method.

6.7.4. NDN performance evaluation

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

NDN (Named Data Networking) is a promising protocol that can help to reduce congestion at Internet scale by putting content at the center of communications instead of hosts. NDN can also natively authenticate transmitted content with a mechanism similar to website certificates that allows clients to assess the original provider. But this security feature comes at a high cost, as it relies heavily on asymmetric cryptography which affects server performance when NDN Data are generated. This is particularly critical for many services dealing with real-time data (VOIP, live streaming, etc.), but current tools are not adapted for a realistic server-side performance evaluation of NDN traffic generation when digital signature is used. We propose a new tool, NDNperf, to perform this evaluation and show that creating NDN packets is a major bottleneck of application performances. On our testbed, 14 server cores only generate $\sim$400 Mbps of new NDN Data with default packet settings. We gave recommendation about the configuration of NDN (packet size, cryptographic function) and proposed practical improvements to the NDN library that all combined can vastly increase the performance of server-side NDN Data generation (x8,5). This work was published in the ACM-ICN conference [22].

7. Bilateral Contracts and Grants with Industry

7.1. 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)

7.2. 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, 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-Define 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, Thales (Elancourt, France)
  - CIFRE PhD (Pierre-Olivier Brissaud, supervised by Isabelle Chrisment and Jérôme François)
  - Anomaly detection in encrypted traffic

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. 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).

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 [12] and [36]).

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

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

8.1.2. Hydradrone FEDER Région Lorraine project

Participants: Adrien Guenard, 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, spinoff from Loria.

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, is providing the use cases and terrain (and business) validation, while Alerion is working on the integration and engineering of the solution.

This second year has been dedicated to the development of the initial controllers for the Hydradrones (smal and large one), and the beginning of the integration of the environmental sensors.

8.1.3. Satelor AME Lorraine regional project

Participants: François Despaux, Lei Mo, Mohamed Tlig, 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 realased. 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 prepared for a further test deployment including several rooms. The second topic is related to improving 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) [33]. The third topic is related to the wireless charging of sensor nodes (PhD work of Lei MO) in order to keeping sensors in perpetual working state. A new direction has been also investigated which consists in using the CSI (channel signal information) of the omnipresent WiFi (IEEE802.11n) as a new generation of contactless sensors. A first test bed of using CSI to measure the respiration rate has been set up.

8.2. National Initiatives

8.2.1. ANR BottleNet

Participants: Isabelle Chrisment [contact], Thibault Cholez, Vassili Rivron, Paul Andrey, Quentin Rouy.

The Quality of Experience (QoE) when accessing the Internet, on which more and more human activities depend, 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 this year with a kick-off on the 1st of 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 it 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.

Our first research question was to evaluate the impact of web advertisement on users' QoE. An interdisciplinary approach was developed at MADYNES, by which we extend the common notion of "quality of information" on free news websites (usually based on journalistic content) to a notion of quality of experience for the user, that takes into account the degraded delivery of information by the multiplication of third party contents. We implemented a measurement tool as a web browser extension and made a dataset by browsing many news websites accessed with and without ad-blockers. The first statistical results retrieved from the dataset show that web-advertisement has a huge negative impact on QoE, for example multiplying the mean page load time by more than one order of magnitude and increasing the variance even more, while adblockers' profiles show faster and more uniform performances. These results have to be further refined but already show that web-advertisement, and more generally third-party content provider, play a huge role in poor Internet QoE and that it is a key parameter to investigate in the project. This study is leading to a structural analysis of the ad regulation mechanisms in the field of web journalism. Adblockers not only upgrades the QoE of visitors, but also contributes to define what "acceptable ads" should be.

This year the following task have been completed:

- Development of a platform to collect QoS & QoE on french news websites (Quentin Rouy, Telecom Nancy student). The first exploratory data collecting campaign measured the impact of Web Advertisement on client QoS, using FatHom plugin for Firefox (a tool from MUSE/Inria, partner of the BottleNet ANR project).
- Implementation of statistical treatment schemes (Paul Andrey, ENSAE student) to correlate QoS, economic models and adblocking effects on news websites.
- Preparation of a systematized measurement campaign on french and international news sites, in order to publish to a large audience.

8.2.2. ANR Doctor

Participants: Thibault Cholez [contact], Thomas Silverston [contact], Xavier Marchal, Cédric Enclos, Elian Aubry, 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. 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.

We presented the whole project at the IRTF Information-Centric Networking Research Group (ICNRG) in January.

This year, we made contributions in three critical points for the deployment of virtualized NDN network: security, performances and interoperability. First, we identified a critical vulnerability in the NDN protocol design that allows an attacker to perform efficient DoS attacks [46] by either self-answering to his own requests or answering to clients before the server. We proposed several remediation strategies to this problem.

On the performance topic, we designed and implemented a tool similar to Iperf, Ndnperf [22][1], that can measure the maximum throughput of a program serving NDN Data. We identified critical limitations that can harm real-time services (live streaming, VOIP, etc.), and proposed several recommendations and improvements that can increase the throughput up to 8 times when combined together.

Finally, we also designed and implemented an HTTP/NDN gateway that can be used to transport web content on an NDN network, thus benefiting from its caching and multicast properties while being totally transparent for the client and the server [47]. Those three contributions were published and demonstrated in the main conference of the domain: ACM ICN.

8.2.3. PIA LAR

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

LAR (Living Assistant Robot) is a PIA (Projet investissement d'avenir) national project getting together Inria (MAIA and MADYNES projects), *Crédit Agricole* (lead), Diatelic and Robotsoft. The aim is to develop an ambient assisted living system for elderly including both sensors and assistant robots. The task of Madynes team is the development of a WSN-based system integrating both sensors of the environment and sensors and actuators embedded on a mobile robot. The research issues include the QoS, energy and mobility management.

This project has ended in March 2016. Some new results are obtained including the use of Cooja simulator for RIOT OS based WSN simulation and an in-depth analysis of some timing inaccuracy problems introduced by MSPSim which is an emulator of MSP430 MCU [27]. A synthesis of our achievements on LAR project is reported in the PhD thesis of Kévin Roussel (http://www.theses.fr/196570603).

8.2.4. FUI HUMA

Participants: Jonathan Arnault, Giulia de Santis, Pierre-Olivier Brissaud, 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 Interministerial) 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 be several months long 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 2016, our contribution focused on defining a clustering technique in order to group individual events into a common one. We applied our technique to darknet data as shown in section 6.2.1. 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 in section 6.2.1. We also technically contribute to the definition of APT scenarios by providing a very stealthy scanning approach (Wiscan described in 6.1.2). 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.

8.2.5. Inria-Orange Joint Lab

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

[1] http://madynes.loria.fr/software/ndnperf_cpp.zip

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.

8.2.6. CNRS-INS2I PEPS NEFAE

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

The need to monitor the increasing proportion of HTTPS traffic while preserving the privacy of users led us to propose a privacy-preserving monitoring framework that allows efficient identification of encrypted traffic (based on full TLS sessions), without relying on any decryption (no HTTPS proxy). It is based on a new set of well-tuned network features to characterise the service inside the encrypted traffic and on machine learning algorithms. The CNRS PEPS founded NEFAE project aims to specifically address the practical challenges toward real time identification of encrypted traffic by developing a next-generation firewall prototype.

This year we first built and made publicly available a new HTTPS dataset[2] (with complete raw data) so that researchers can compare their identification algorithms. We also improved our HTTPS monitoring framework to allow real-time identification of HTTPS services with only a few data packets instead of the full TLS session. We show better performances that the related work in all dimensions: better accuracy, earlier decision and more fine-grained identification). A running prototype is also under development to evaluate the scalability and overhead of our solution.

8.2.7. CNRS-INS2I PEPS SURF

Participants: Abdelkader Lahmadi [contact], Jérôme François, Isabelle Chrisment.

The SURF project, funded by the CNRS PEPS program, addresses the challenge of a developing a methodology for the joint modelling and the analysis of the Cyber security and the safety of industrial systems in the context of the factory of the future. The project involves partners from the Heudiasyc Laboratory of the University of Technology of Compiègne (UTC), the CRAN laboratory and the Inria Madynes team. The goal of the project is to make a joint effort from safety and cyber security communities to address the challenges of a joint modelling of industrial systems while including attacks, vulnerabilities and failures. During the year 2016, with the partners of the project, we have mainly identified the key challenges regarding this issue where we identified the common models, metrics and analysis methods that should be built. We have also organized a scientific day (http://surf.loria.fr) with many industrials (EDF, PSA and Sentryo) and academic to share with them our work and clearly identify the requirement and experience regarding this issue. This short term project is ended by this year, however a consortium is established for further long term projects (ANR, FUI or H2020) to address the identified challenge of a joint analysis of the cyber security and the safety of industrial control systems.

8.2.8. 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

[2] http://betternet.lhs.loria.fr/datasets/https/

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 will cover the fundamental concepts, architectures and protocols of the domain, as well as their evolution in the context of future Internet, and will include practical labs and exercises using widely-used tools and technologies.

8.2.9. Technological Development Action (ADT)

8.2.9.1. ADT UASS

The goal of this ADT is while still providing 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 tutoring 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.

8.2.9.2. ADT VERTEX

This ADT started on 2016 and will end on 2018. The Madynes project is a major partner funded at the level of 120k€. ADT VERTEX buildt 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. Already developed prototypes are also being consolidated, and the necessary improvements to user management and tracking are also being performed.

8.2.9.3. ADT COSETTE

This ADT started on 2013 and is endind on 2016. The Madynes project is the only partner funded at the level of 120k€. ADT COSETTE, for *COherent SET of Tools for Experimentation* aims at developing or improving a tool suite for experimentation at large scale on testbeds such as Grid'5000. Specifically, we will work on (1) the development of Ruby-CUTE, a library gathering features useful when performing such experiments; (2) the porting of Kadeploy, Distem and XPFlow on top of Ruby-CUTE; (3) the release of XPFlow, developed in the context of Tomasz Buchert's PhD; (4) the improvement of the Distem emulator to address new scientific challenges in Cloud and HPC. E. Jeanvoine (SED) is delegated in the Madynes team for the duration of this project. A subsequent project is planned to start at the end of 2016 (ADT SDT).

8.2.9.4. 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 (https://github.com/RIOT-OS/RIOT/pull/5941; https://github.com/RIOT-OS/RIOT/pull/5942; https://github.com/RIOT-OS/RIOT/pull/5949; https://github.com/RIOT-OS/RIOT/pull/5950; https://github.com/RIOT-OS/RIOT/pull/6069; https://github.com/RIOT-OS/RIOT/pull/6072). Based on these generic functions, we first contributed to the functionality and performance improvement of an universal example MAC protocol (Lw-MAC) (https://github.com/RIOT-OS/RIOT/pull/5941). We then implemented iQueue-MAC, which is a robust, energy efficient and traffic adaptive MAC protocol (https://github.com/RIOT-OS/RIOT/pull/5618). Currently, we have finished to implement most of the designed features of iQueue-MAC, such as the low duty-cycle scheme, the adaptive slots allocation scheme and the multi-channel operation. Experimental results collected from samr21-Xplained-pro boards showed that iQueue-MAC is robust and has a extremely low packet drop ratio, even when interference is strong.

8.2.10. Inria Project Lab

8.2.10.1. IPL BetterNet

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

The Inria Project Lab BetterNet (https://project.inria.fr/betternet) 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 the IPL and in particular Isabelle Chrisment who coordinates the project. Several actions have already been done over the first months:

- Organization of the Kick-Off the 19th November in Paris;
- Recruitment of a shared PhD with SPYRALS (Inria/University of Lille3) in order to develop probes and collecting platform;
- Servers installation in LHS (High Security Laboratory) for the hosting of the different BottleNet and BetterNet data collection and opendata platforms;
- Preparation of small and middle scale QoE and QoS data collection with users. Conception of incentives and rewards (value added services).

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

8.3.1.1. Flamingo

Title: Management of the Future Internet

Programm: FP7

Duration: November 2012 - December 2016

Coordinator: University Twente

Partners:

Iminds Vzw (Belgium),
Jacobs University Bremen Ggmbh (Germany),
University College London (United Kingdom),
Université de Lorraine (France),
Universitaet Der Bundeswehr Muenchen (Germany),
Universitat Politecnica de Catalunya (Spain),
Universiteit Twente (Netherlands),
Universitaet Zuerich (Switzerland)

Inria contact: Jérôme François

The goals of FLAMINGO are (a) to strongly integrate the research of leading European research groups in the area of network and service management, (b) to strengthen the European and worldwide research in this area, and (c) to bridge the gap between scientific research and industrial application.

In 2016, our research activities in Flamingo have been focused on (a) the analysis and evaluation of OpenFlow message usage for security applications, in particular to enable fast deployment and reconfiguration of mitigation technique (6.2.4) in cooperation with Universitaet Der Bundeswehr Muenchen; (b) passive monitoring of Internet-of-Things using the RPL protocol in cooperation with the Jacobs University Bremen; (c) monitoring of HTTPS traffic to identify user services without necessity of decrypting (6.1.4) and (d) low-footprint Internet wide scanning using our WISCAN software developed last year.

We have pursued leading the standardization activities of the project (WP leader).

8.3.2. Collaborations in European Programs, Except FP7 & H2020

8.3.2.1. 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.

8.4. International Initiatives

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

8.4.1.1. IoT4D

Title: Internet of Things for Developping countries

International Partner (Institution - Laboratory - Researcher):

UY (Cameroon) - MASECNeSS - Thomas DJOTIO NDIE

Start year: 2016

We want connect wireless sensors networks to the Internet through gateways. Wireless network should have several acessible 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 this perticular context, with unreliable communications and equipments that are easily disturbed by the environment

8.4.1.2. 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

Start year: 2016

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

Networking is deeply evolving with the rise of programmability and virtualization. The concept of SDI (Software-Defined Infrastructure) has emerged from SDN (Software-Defined Networking) and NFV (Network Function Virtualization) making thus the configuration of the network highly dynamic and adaptable in real-time. However, new methods and tools have to be defined to properly monitor and configure this type of infrastructure. Current works are mainly limited to apply former approaches of traditional network but do not exploit the novel capabilities offered by these technologies. The goal of the associate team is thus to define methodologies taking benefit of them for an efficient monitoring and use of SDI resources while investigating security issues it brings.

8.4.1.3. STIC-AmSud AKD Project

Participants: Rémi Badonnel [contact], Olivier Festor, Gaetan Hurel, Amedeo Napoli.

The AKD project, funded by the STIC-AmSud Program, addresses the challenge of autonomic knowledge discovery for security vulnerability prevention in self-governing systems. The partners include Federal University of Rio Grande do Sul (UFRGS, Brazil), Republic University of Uruguay (INCO, Uruguay), Technical University of Federico Santa Maria (UTFSM, Chile), and Inria (Orpailleur, Madynes). Computer vulnerabilities constitute one of the main entry points for security attacks, and therefore, vulnerability management mechanisms are crucial for any computer systems. However autonomic mechanisms for assessing and remediating vulnerabilities can degrade the performance of the system and might contradict existing operational policies. In that context, this project focuses on the design of solutions able to pro-actively understand the behavior of systems and networks, in order to prevent vulnerable states. For that purpose, our work concerns more specifically the exploitation and integration of knowledge discovery techniques within autonomic systems for providing intelligent self-configuration and self-protection. It also investigates the building of flexible and dynamic security management mechanisms taking benefits from software-defined methods and techniques.

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

Rémi Badonnel was member of the organizing committee for the following conferences: IEEE International Conference on Network Softwarization (IEEE NetSoft 2016), IEEE/IFIP/In Assoc. with ACM SIGCOMM International Conference on Network and Service Management (IEEE/IFIP/In Assoc. with ACM SIGCOMM CNSM 2016), IEEE/IFIP International Symposium on Integrated Network Management (IEEE/IFIP IM 2017).

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

Rémi Badonnel was TPC co-chair for the following conferences: the Experience Track of the IFIP/IEEE Network Operations and Management Symposium (IFIP/IEEE NOMS 2016), IFIP/IEEE International Workshop of Management of the Future Internet (IFIP/IEEE ManFI 2016), IFIP International Conference on Autonomous Infrastructure, Management and Security (IFIP AIMS 2016).

Isabelle Chrisment was TPC co-chair of the first IFIP Internet of People Workshop co-located with IFIP Networking 2016. She was member of the steering committee for RESSI'16 (Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information).

Olivier Festor was TPC co-chair of ACM/IEEE/IFIP Conference on Netwrk and Service Management (CNSM) 2016. He is also member of the steering committee (NISC) that coordinates the main conferences in network and service management (IM, NOMS, CNSM and AIMS). He was also Tutorial chair of IEEE Netsoft 2016 and workshop co-chair at IEEE/IFIP NOMS'2016.

9.1.2.2. Member of the Conference Program Committees

Rémi Badonnel: IFIP International Conference on Autonomous Infrastructure, Management and Security (IFIP AIMS 2016) ; IFIP/IEEE International Conference on Network and Service Management (IFIP/IEEE CNSM 2016) ; IEEE Global Information Infrastructure and Networking Symposium (IEEE GIIS 2016) ; IEEE Global Communications Conference (IEEE GLOBECOM - SAC 2016) ; IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM 2017).

Thibault Cholez: 2nd IEEE International Workshop on Security Testing and Monitoring (STAM 2016, IEEE ICDCS Workshop)

Isabelle Chrisment: IFIP International Conference on Autonomous Infrastructures, Management and Security (IFIP AIMS'16) ; Rencontres Francophones sur la Conception de Protocoles, l'évaluation de Performance et l'Expérimentation Aspects Algorithmiques de Télécommunications (CoResl'16) ; IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2016) ; IEEE/IFIP International Symposium on Network Operations and Management (IEEE/IFIP NOMS'16).

Oliver Festor: IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM'2017) ; IEEE/IFIP Network Operations and Management Symposium 2016 ; IEEE Netsoft 2016 ; IEEE Asia Pacific NOMS'2016.

Jérôme François: IFIP International Conference on Autonomous Infrastructure, Management and Security (IFIP AIMS 2016) ; IEEE Global Information Infrastructure and Networking Symposium (IEEE GIIS 2016) ; Principles, Systems and Applications of IP Telecommunications (IPTComm'16) ; IFIP/IEEE International Workshop on Management of SDN and NFV Systems (IFIP/IEEE ManSDN 2016) ; Asia-Pacific Network Operations and Management Symposium (APNOMS 2016); IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM 2017).

Abdelkader Lahmadi: IFIP International Conference on Autonomous Infrastructure, Management and Security (IFIP AIMS 2016), PhD workshop ; Asia-Pacific Network Operations and Management Symposium (APNOMS 2016); IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM 2017); IEEE/IFIP International Workshop on Management of the Future Internet (ManFI 2016, held as part of IEEE/IFIP NOMS 2016); IEEE Conference on Network Softwarization (IEEE NetSoft 2016).

Ye-Qiong Song: IEEE International Workshop on Factory Communication Systems (WFCS 2016); IEEE International Conference on Communications and Networking (ComNet 2016) ; IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2016) ; 24th International Conference on Real-Time Networks and Systems (RTNS 2016) ; IEEE International conference on Telecommunications (ICT-2016) ; IFIP Wireless and Mobile Networking Conference (WMNC 2016).

Laurent Ciarletta: International Program Comittee, IEEE CSS / RAS International Conference on Unmanned Aircraft Systems ICUAS 2016.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

Rémi Badonnel is Associate Editor for the Wiley International Journal of Network Management (IJNM).

Olivier Festor is an associate editor of IEEE Transactions on Networks and Systems Management (TNSM).

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

9.1.3.2. 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).

Thibault Cholez: Journal of Communications and Networks, Elsevier Computer Networks, IEEE Transactions on Network and Service Management, Elsevier Computers & Security, IEEE Global Communications Conference, IFIP/IEEE International Symposium on Integrated Network Management

Isabelle Chrisment: IEEE Transactions on Network and Service Management (IEEE TNSM), IEEE Communications Magazine (COMMAG), Wiley Security and Communication Networks (SCN).

Jérôme François: IEEE Transactions on Network and Service Management (IEEE TNSM), Springer Journal of Network and Systems Management, Elsevier Computer Networks Journal

Abdelkader Lahmadi: IEEE Transactions on Network and Service Management (IEEE TNSM); IEEE Communications Magazine (COMMAG); Springer Journal of Network and Systems Management (JNSM); Elsevier Journal of Computer Communications (COMCOM); Elsevier Journal of Engineering Applications of Artificial Intelligence (EAAI).

Ye-Qiong Song: Elsevier Computers and Electrical Engineering journal, Elsevier Ad hoc network journal, Journal of Real-time systems (Springer), IEEE Transactions on Industrial Informatics.

9.1.4. Invited Talks

Thibault Cholez:

- RESSI 2016, Toulouse: "Efficiently Bypassing SNI-based HTTPS Filtering"
- IRTF ICNRG, Paris: "Challenges and directions for the security management of ICN services"

Isabelle Chrisment:

- US-EU Workshop on the Next Generation Internet of Things, March 30-April, 2016, USC, Los Angeles, USA. "Security and Monitoring of (Every)Things"

Jérôme François:

- IRTF NMLRG (IETF 95), Buenos Aires, Argentina: "HTTPS Traffic Classification"
- IRTF NMLRG (colocated with EuCNC), Athens, Greece, " NML in Inria High Security Lab: overview and datasets"
- IRTF NMLRG (IETF 96), Berlin, Germany: "Malicious Domains: Automatic Detection with DNS Traffic Analysis"

Abdelkader Lahmadi:

- i-NOVIA (Salon of Nouvelle Technologies), Strasbourg, "Cybersecurity: monitoring and defense", 5 October 2016

9.1.5. Scientific Expertise

Laurent Ciarletta serves as expert for the 2016 ANR Generic call.

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

Ye-Qiong Song serves as reviewer for ANRT to evaluate a CIFRE PhD proposition.

Ye-Qiong Song serves as expert for "Fonds de recherche nature et technologies, Quebec".

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Rémi Badonnel is heading the Telecommunications, Networks and Services 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 and ENSEM engineering schools.

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).

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

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

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

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

Laurent Ciarletta 250 hours - M1, M2 - Networks and Services, Interactive Computing, Pervasive Comuting, Software Design and Programming, ARTEM - Mines Nancy - Ecole Nationale Superieure des Mines de nancy - Engineering school, Université de Lorraine, France

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

Abdelkader Lahmadi 280 hours - L1, M1, M2 and Master Degree in Computer Science - Algorithms and Java programming, C language programming, Distributed algorithms, Sensor networks programming -ENSEM Engineering school, Université de Lorraine, France.

Ye-Qiong Song 230 hours - L1, M1, M2 Engineering degree and Master Degree in Computer Science - Algorithms and Java programming, Databases, Networking, Sensor networks - ENSEM - Engineering school, Université de Lorraine, France.

9.2.2. Supervision

9.2.2.1. PhD in progress in team

Elian Aubry, *Using Software Defined Network to manage Content Centric Networks*, since October 2013, supervised by Isabelle Chrisment & Thomas Silverston.

Pierre-Olivier Brissaud, *Anomaly detection in encrypted traffic*, since July 2016, supervised by Isabelle Chrisment, Jérôme François & Olivier Bettan (Thales)

Paul Chaignon, *Monitoring of SDN networks*, since July 2016, supervised by Olivier Festor, Jérôme François & Kahina Lazri (Orange Labs)

Maxime Compastie, *Software-Defined Security for the Cloud*, since Dec 2015, supervised by Olivier Festor & Rémi Badonnel.

Giulia De Santis, *Modelling and Analysis of Complex and Targeted Cyberattacks*, since October 2015, Olivier Festor & Abdelkader Lahmadi.

Meihui Gao, *Optimization models and methods for Network Functions Virtualization architectures*, since Nov 2015, supervised by Ye-Qiong Song & Bernardetta Addis.

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

Julien Vaubourg, *IP network models and simulators integration with DEVS for co-simulation of CPS*, since Oct. 2013, supervised by Vincent Chevrier & Laurent Ciarletta.

Thomas Paris, *Complex systems modeling using composition*, since Oct. 2015, supervised by Vincent Chevrier & Laurent Ciarletta.

Petro Aksonenko, *Optilized method of Calibration, Alignement and Advanced Attitude Algorithms for Strapdown Inertial Navigation Systems*, since Oct. 2016, supervised by Patrick Henaff, Anton Popov (KPI University) & Laurent Ciarletta

Patrick-Olivier Kamgue, *Routing management in WSNs*, since Jun 2012, supervised by Emmanuel Nataf & Olivier Festor in France, Thomas Djotio in Cameroun.

Daishi Kondo, *New Networking Architecture through Virtualization*, since September 2015, supervised with Olivier Perrin (EPI COAST) & Thomas Silverston.

Xavier Marchal, *Secure operation of virtualized Named Data Networks traffic*, since December 2015, supervised by Olivier Festor & Thibault Cholez.

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

Evangelia Tsiontsiou, *Multiconstrained QoS routing for wireless sensors networks with applications to smart space for ambient assisted living*, since Oct 2013, supervised by Ye-Qiong Song & Bernardetta Addis.

Shbair Wazen, *Service-level Monitoring of HTTPS*, since December 2013, supervised by Isabelle Chrisment & Thibault Cholez.

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

9.2.2.2. PhD defended in team

- [1] Tomasz Buchert, *Managing large-scale, distributed systems research experiments with control-flows*, *Université de Lorraine*, January 2016, supervised by Jens Gustedt & Lucas Nussbaum.
- Anthea Mayzaud, *Monitoring and Security for the Internet of Things* [3], *Université de Lorraine*, October 2016, supervised by Isabelle Chrisment & Rémi Badonnel.
- Kévin Roussel, *Dynamic management of QoS and energy in heterogeneous sensor networks for e-health applications* [4], June 2016, supervised by Ye-Qiong Song & Olivier Zendra.

9.2.3. Juries

Team members participated to the following Ph.D. defense committees in Computer Science if no other indication:

- Femke De Backere, in Computer Science from Ghent University, Belgium. Title: Design and Management of Pervasive eCare Services, June 2016 – (Rémi Badonnel as reviewer).
- Pasquale Puzio, PhD in Computer Science from TELECOM ParisTech, Sophia Antipolis, France. Title: Deduplication of Encrypted Data in Cloud Computing, February 2016 – (Isabelle Chrisment as examiner).
- Ziad Ismail, PhD in Computer Science from TELECOM ParisTech, Paris, France. Title: Optimal Defense Strategies to Improve the Security and Resilience of Smart Grids, April 2016 – (Isabelle Chrisment as reviewer).
- Erwan Godefroy, PhD in Computer Science from CentraleSupélec, Rennes, France. Title: *Définition et évaluation d'un mécanisme de génération de règles de corrélation liées à l'environnement*, September 2016 – (Isabelle Chrisment as president).
- Hiep Huu Nguyen, PhD in Computer Science from Université de Lorraine, Nancy, France. Title: Social Graph Anonymization, November 2016 – (Isabelle Chrisment as president).
- Chakadkit Thaenchaikun, PhD in Computer Science from Université de Toulouse, France. Title: Economie d'énergie en réseau filaire: Ingéniérie de trafic et mise en veille, November 2016 – (Isabelle Chrisment as reviewer).
- Kim Thuat Nguyen, PhD in Computer Science from Télécom SudParis, France. Title: Protocoles de sécurité efficaces pour les réseaux de capteurs IP sans-fil et l'Internet des Objets, December 2016 – (Isabelle Chrisment as reviewer).
- Mohamed Sabt, PhD in Computer Science from Université de Technologie de Compiègne, France. Title: Outsmarting Smartphones - Trust based on Provable Security and Hardware Primitives in Smartphones Architectures, December 2016 – (Isabelle Chrisment as examiner).

[3] registration not fully completed
[4] http://www.theses.fr/2016LORR0051

- Michal Krol, PhD. in Computer Science from University of Grenoble, Frace. Title: Routing in wireless sensor networks, March 2016 – (Olivier Festor as reviewer).
- Marc Bruyère, PhD. in Computer Science from University of Toulouse 3 - Paul Sabatier, France. Title: An outright open source approach for simple andpragmatic Internet eXchange, July 2016 – (Olivier Festor as reviewer).
- Ahmed Bouchami, PhD. in Computer Science from Universié de Lorraine. Title: Sécurité des ressources collaboratives dans les réseaux sociaux d'entreprise, July 2016. – (Olivier Festor as President).
- Benjamin Baron, PhD. in Computer Science from Pierre et Marie Curie Paris VI - Sorbonne Universités, France. Title: *Transport intermodalde données massives pour le délestage des réseaux d'infrastructure*, October 2016 – (Olivier Festor as examiner).
- Messaoud Aouadj, PhD. in Computer Science from University of Toulouse 3 - Paul Sabatier, France. Title: *AirNet: le modèle de virtualisation Edge-Fabric comme plan de contrôle poru les réseaux programmables*, November 2016. – (Olivier Festor as reviewer).
- Tiphaine Viard, PhD. in Computer Science from Pierre et Marie Curie - Sorbonne Universités, France. Title: *Flots de liens pour la modélisation d'interactions temporelles et application à l analyse de trafic IP*, September 2016 – (Olivier Festor as reviewer).
- Christoph Neumann, HDR in Computer Science from University of Rennes 1, France. Title: Contributions to Content Placement,Load-balancing and Caching: System Design and Security, November – 2016 (Olivier Festor as reviewer).
- Nadjib Ait Saadi, HDR in COMputer Science from University Paris Est Créteil, France. Title: From Sensors to Data Centers: Optimization of Deployment, Resource Allocation and Reliability, July 2016 – (Olivier Festor as President).
- Promethee Spathis, HDR in Computer Science from Pierre et Marie Curie - Sorbonne Universités, France. Title: Information DeliveryPast Struggles and New Directions, December 2016 – (Olivier Festor as reviewer).
- Hassan Said MOUSTAFA HARB, PhD. Université de Franche-Comté, France. Title: Energy Efficient Data Handling and Coverage for Wireless Sensor Networks, July 2016 – (Ye-Qiong Song as examiner).
- d'Abderrahmen Belfkih, PhD. Université du Havre, Title Contraintes temporelles dans les bases de données de capteurs sans fil, October 2016 – (Ye-Qiong Song as reviewer).
- Kawther Hassine, Ph.D. in ICT from Université de Carthage - SUPCOM Tunis. Title: Performance study of future wireless networks IEEE802.11 xy, December 2016 – (Ye-Qiong Song as reviewer).
- Lemia Louail, PhD. Université de Franche-Comté, Title: Approches cross-layer pour l'optimisation de la latence des communications dans les réseaux de capteurs sans fil, December 2016 – (Ye-Qiong Song as reviewer).
- Ahlem Mifdaoui, HDR. Université de Toulouse, Title: Contributions to Performance Analysis of Networked Cyber-Physical Systems, December 2016 – (Ye-Qiong Song as reviewer).

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] T. BUCHERT. *Managing large-scale, distributed systems research experiments with control-flows*, Université de Lorraine, January 2016, https://tel.archives-ouvertes.fr/tel-01273964

Articles in International Peer-Reviewed Journals

[2] A. MAYZAUD, R. BADONNEL, I. CHRISMENT. *A Taxonomy of Attacks in RPL-based Internet of Things*, in "International Journal of Network Security", May 2016, vol. 18, n^{o} 3, pp. 459 - 473,, https://hal.inria.fr/hal-01207859

[3] Y. QI, P. CHENG, J. BAI, J. CHEN, G. ADRIEN, Y.-Q. SONG, Z. SHI. *Energy-Efficient Target Tracking by Mobile Sensors With Limited Sensing Range*, in "IEEE Transactions on Industrial Electronics", November 2016, vol. 63, n^{o} 11, 12 p. [*DOI :* 10.1109/TIE.2016.2584000], https://hal.inria.fr/hal-01403761

Articles in National Peer-Reviewed Journals

[4] M. TLIG, O. BUFFET, O. SIMONIN. *Intersections intelligentes pour le contrôle de véhicules sans pilote : coordination locale et optimisation globale*, in "Revue des Sciences et Technologies de l'Information - Série RIA : Revue d'Intelligence Artificielle", 2016, https://hal.inria.fr/hal-01330354

Invited Conferences

[5] L. NUSSBAUM. *Chameleon, CloudLab, Grid'5000: What will the ultimate testbed look like?*, in "Grid'5000 Winter School 2016", Grenoble, France, February 2016, https://hal.inria.fr/hal-01274298

[6] L. NUSSBAUM. *Deployment of Cloud stacks on Grid'5000*, in "GEFI Workshop", Brussels, Belgium, April 2016, https://hal.inria.fr/hal-01313210

[7] L. NUSSBAUM. *Federating Grid'5000*, in "GEFI Workshop", Brussels, Belgium, April 2016, https://hal.inria.fr/hal-01313207

[8] L. NUSSBAUM. *SDN/NFV experiments on Grid'5000*, in "GEFI Workshop", Brussels, Belgium, April 2016, https://hal.inria.fr/hal-01313204

[9] L. NUSSBAUM. *Supporting Big Data experiments on Grid'5000*, in "GEFI Workshop", Brussels, Belgium, April 2016, https://hal.inria.fr/hal-01308370

International Conferences with Proceedings

[10] E. AUBRY, T. SILVERSTON, I. CHRISMENT. *Croissance Verte dans NDN: Déploiement des Content Stores*, in "ALGOTEL 2016 - 18èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications", Bayonne, France, ALGOTEL 2016 - 18èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications, May 2016, https://hal.archives-ouvertes.fr/hal-01304444

[11] E. AUBRY, T. SILVERSTON, I. CHRISMENT. *Green Growth in NDN: Deployment of Content Stores*, in "LANMAN 2016 - IEEE International Symposium on Local and Metropolitan Area Networks", Rome, Italy, Local and Metropolitan Area Networks (LANMAN), 2016 IEEE International Symposium on, IEEE, June 2016 [*DOI :* 10.1109/LANMAN.2016.7548850], https://hal.archives-ouvertes.fr/hal-01405820

[12] A. BELKADI, D. THEILLIOL, L. CIARLETTA, J.-C. PONSART. *Robust flocking control design for a fleet of autonomous agents*, in "3rd Conference on Control and Fault-Tolerant Systems, SysTol 2016", Barcelone, Spain, September 2016, https://hal.archives-ouvertes.fr/hal-01348138

[13] B. CAMUS, V. GALTIER, M. CAUJOLLE, V. CHEVRIER, J. VAUBOURG, L. CIARLETTA, C. BOURJOT. *Hybrid Co-simulation of FMUs using DEV&DESS in MECSYCO*, in "Symposium on Theory of Modeling & Simulation - DEVS Integrative M&S Symposium", Pasadena, CA, United States, Proceedings of the Symposium on Theory of Modeling & Simulation - DEVS Integrative M&S Symposium (TMS/DEVS 16), SCS/ACM (2016), April 2016, pp. 568-575, https://hal.archives-ouvertes.fr/hal-01307616

[14] L. CIARLETTA, L. FEJOZ, A. GUENARD, N. NAVET. *Development of a safe CPS component: the hybrid parachute, a remote termination add-on improving safety of UAS*, in "ERTS 2016 - 8th European Congress on Embedded Real Time Software and Systems", Toulous, France, January 2016, 10 p. , https://hal.inria.fr/hal-01251305

[15] L. CIARLETTA, T. GURRIET. *Towards a Generic and Modular Geofencing Strategy for Civilian UAVs*, in "2016 International Conference on Unmanned Aircraft Systems", Arlington, VA, United States, 2016 ICUAS Proceedings, June 2016, n^{o} 9781467393355, https://hal.inria.fr/hal-01398431

[16] M. COMPASTIÉ, R. BADONNEL, O. FESTOR, R. HE, M. KASSI LAHLOU. *A Software-Defined Security Strategy for Supporting Autonomic Security Enforcement in Distributed Cloud*, in "IEEE International Conference on Cloud Computing Technology and Science (CloudCom'16), PhD Symposium", Luxembourg, Luxembourg, December 2016, 4 p. , https://hal.inria.fr/hal-01399458

[17] M. COUDRIAU, A. LAHMADI, J. FRANCOIS. *Topological Analysis and Visualisation of Network Monitoring Data: Darknet case study*, in "8th IEEE International Workshop on Information Forensics and Security - WIFS 2016", Abu Dhabi, United Arab Emirates, Information Forensics and Security, IEEE, December 2016, https://hal.inria.fr/hal-01403950

[18] G. DE SANTIS, A. LAHMADI, J. FRANCOIS, O. FESTOR. *Modeling of IP scanning activities with Hidden Markov Models: Darknet case study*, in "8th IFIP International Conference on New Technologies, Mobility and Security", Larnaca, Cyprus, International Conference on New Technologies, Mobility and Security (NTMS), November 2016, https://hal.inria.fr/hal-01404127

[19] L. DOLBERG, J. FRANCOIS, S. R. CHOWDHURY, R. AHMED, R. BOUTABA, T. ENGEL. *A Generic Framework to Support Application-Level Flow Management in Software-Defined Networks*, in "Conference on Network Softwarization (Netsoft)", Seoul, South Korea, IEEE, June 2016, https://hal.inria.fr/hal-01310574

[20] J. FRANÇOIS, A. LAHMADI, V. GIANNINI, D. CUPIF, F. BECK, B. WALLRICH. *Optimizing Internet Scanning for Assessing Industrial Systems Exposure*, in "7th International Workshop on TRaffic Analysis and Characterization", Paphos, Cyprus, TRAC 2016 - 7th International Workshop on TRaffic Analysis and Characterization, September 2016 [*DOI :* 10.1109/IWCMC.2016.7577111], https://hal.inria.fr/hal-01371674

[21] F. GREFF, E. DUJARDIN, A. SAMAMA, Y.-Q. SONG, L. CIARLETTA. *A Symbiotic Approach to Designing Cross-Layer QoS in Embedded Real-Time Systems*, in "8th European Congress on Embedded Real Time Software and Systems (ERTS 2016)"", Toulouse, France, January 2016, https://hal.inria.fr/hal-01242068

[22] X. MARCHAL, T. CHOLEZ, O. FESTOR. *Server-side performance evaluation of NDN*, in "3rd ACM Conference on Information-Centric Networking (ACM-ICN'16)", Kyoto, Japan, ACM, September 2016, pp. 148 - 153 [*DOI :* 10.1145/2984356.2984364], https://hal.inria.fr/hal-01386777

[23] A. MAYZAUD, R. BADONNEL, I. CHRISMENT. *Detecting Version Number Attacks in RPL-based Networks using a Distributed Monitoring Architecture*, in "IEEE/IFIP/In Assoc. with ACM SIGCOMM International Conference on Network and Service Management (CNSM'12)", Montreal, Canada, October 2016, 9 p. , https://hal.inria.fr/hal-01399432

[24] A. MAYZAUD, A. SEHGAL, R. BADONNEL, I. CHRISMENT, J. SCHÖNWÄLDER. *Using the RPL Protocol for Supporting Passive Monitoring in the Internet of Things*, in "IEEE/IFIP Network Operations and Management Symposium", Istanbul, Turkey, April 2016, https://hal.inria.fr/hal-01247297

[25] T. PARIS, A. TAN, V. CHEVRIER, L. CIARLETTA. *Study about decomposition and integration of continuous systems in discrete environment*, in "Annual Simulation Symposium (ANSS)", Pasadena, United States, Proceedings of the Annual Simulation Symposium (ANSS) 2016, April 2016, https://hal.inria.fr/hal-01256969

[26] V. RIVRON, M. I. KHAN, S. CHARNEAU, I. CHRISMENT. *Exploring Smartphone Application Usage Logs with Declared Sociological Information*, in "Social computing and networking", Atlanta, United States, SocialCom 2016 : The 9th IEEE International Conference on Social Computing and Networking, IEEE, October 2016 [*DOI :* 10.1109/BDCLOUD-SOCIALCOM-SUSTAINCOM.2016.49], https://hal.inria.fr/hal-01378795

[27] K. ROUSSEL, Y.-Q. SONG, O. ZENDRA. *Using Cooja for WSN Simulations: Some New Uses and Limits*, in "EWSN 2016 — NextMote workshop", Graz, Austria, K. ROEMER (editor), EWSN 2016 — NextMote workshop, Junction Publishing, February 2016, 319324 p. , https://hal.inria.fr/hal-01240986

[28] C. RUIZ, J. EMERAS, E. JEANVOINE, L. NUSSBAUM. *Distem: Evaluation of Fault Tolerance and Load Balancing Strategies in Real HPC Runtimes through Emulation*, in "CCGRID - 16th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing", Cartagena, Colombia, May 2016, https://hal.inria.fr/hal-00949762

[29] S. SEEBER, R. GABI DREO, G. HUREL, R. BADONNEL. *Analysis and Evaluation of OpenFlow Message Usage for Security Applications*, in "IFIP International Conference on Autonomous Infrastructure, Management and Security (IFIP AIMS 2016)", Munich, Germany, Springer - Lecture Notes of Computer Science, June 2016, 12 p. , https://hal.inria.fr/hal-01399439

[30] W. M. SHBAIR, T. CHOLEZ, J. FRANÇOIS, I. CHRISMENT. *A Multi-Level Framework to Identify HTTPS Services*, in "IEEE/IFIP Network Operations and Management Symposium (NOMS 2016)", Istanbul, Turkey, IEEE, April 2016, pp. p240-248 [*DOI :* 10.1109/NOMS.2016.7502818], https://hal.inria.fr/hal-01273160

[31] W. M. SHBAIR, T. CHOLEZ, J. FRANÇOIS, I. CHRISMENT. *Improving SNI-based HTTPS Security Monitoring*, in "Second IEEE International Workshop on Security Testing and Monitoring", Nara, Japan, ICDCS 2016 - Workshops of the 36th IEEE International Conference on Distributed Computing Systems., IEEE, June 2016, 6 p. , https://hal.inria.fr/hal-01349710

[32] S. SIGNORELLO, R. STATE, J. FRANCOIS, O. FESTOR. *NDN.p4: Programming Information-Centric Data-Planes*, in "International Workshop on Open-Source Software Networking (OSSN), IEEE International Conference on Network Softwarization", Seoul, South Korea, June 2016, https://hal.inria.fr/hal-01310575

[33] E. TSIONTSIOU, B. ADDIS, Y.-Q. SONG, A. CESELLI. *Optimal Probabilistic Energy-Aware Routing for Duty-Cycled Wireless Sensor Networks*, in "8th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2016)", Larnaca, Cyprus, November 2016, https://hal.inria.fr/hal-01404169

[34] J. VAUBOURG, V. CHEVRIER, L. CIARLETTA, B. CAMUS. *Co-Simulation of IP Network Models in the Cyber-Physical Systems Context, using a DEVS-based Platform*, in "Communications and Networking Simulation Symposium", Pasadena, United States, Proceedings of the Communications and Networking Simulation Symposium, ACM, 2016, Society for Computer Simulation International, https://hal.archives-ouvertes.fr/hal-01256907

National Conferences with Proceedings

[35] A. SAIF, L. NUSSBAUM. *Performance Evaluation of NFS over a Wide-Area Network*, in "COMPAS - Conférence d'informatique en Parallélisme, Architecture et Système", Lorient, France, July 2016, https://hal.inria.fr/hal-01327272

Conferences without Proceedings

[36] A. BELKADI, L. CIARLETTA, D. THEILLIOL. *UAVs fleet control design using distributed particle swarm optimization: A leaderless approach*, in "International Conference on Unmanned Aircraft Systems, ICUAS 2016", Arlington, VA, United States, June 2016, pp. 364-371 [*DOI :* 10.1109/ICUAS.2016.7502679], https://hal.archives-ouvertes.fr/hal-01382063

[37] D. I. MAXIM, R. DAVIS, L. I. CUCU-GROSJEAN, A. EASWARAN. *Probabilistic Analysis for Mixed Criticality Scheduling with SMC and AMC*, in "WMC 2016", Porto, Portugal, November 2016, https://hal.archives-ouvertes.fr/hal-01416310

[38] L. NUSSBAUM. *Towards reproducibility of experiments*, in "Grid'5000 Winter School 2016 – Grid'5000 Scientific Advisory Board meeting", Grenoble, France, February 2016, https://hal.inria.fr/hal-01274293

Books or Proceedings Editing

[39] R. BADONNEL, R. KOCH, A. PRAS, M. DRASAR, B. STILLER (editors). *Management and Security in the Age of Hyperconnectivity - Proceedings of the 10th IFIP International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2016)*, Lecture Notes in Computer Science 9701, Springer - Lecture Notes of Computer Science, Munich, Germany, June 2016, https://hal.inria.fr/hal-01399447

[40] J. WON-KI HONG, F. D. TURCK, J. KANG, H. CHOO, R. BADONNEL, B.-Y. CHOI, K. MYUNGSUP (editors). *Softwarization of Networks, Clouds, and Internet of Things - Proceedings of the 2nd IEEE International Conference on Network Softwarization (NetSoft 2016)*, Proceedings of the 2nd IEEE International Conference on Network Softwarization (NetSoft 2016), June 2016, https://hal.inria.fr/hal-01399452

Research Reports

[41] B. CAMUS, V. GALTIER, M. CAUJOLLE, V. CHEVRIER, J. VAUBOURG, L. CIARLETTA, C. BOURJOT. *Hybrid Co-simulation of FMUs using DEV&DESS in MECSYCO*, Université de Lorraine, CNRS, Inria, LORIA, UMR 7503 ; CentraleSupélec UMI GT-CNRS 2958 Université Paris-Saclay ; EDF - R&D MIRE/R44, January 2016, https://hal.inria.fr/hal-01256738

[42] 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

[43] C. RUIZ, E. JEANVOINE, L. NUSSBAUM. *Porting the Distem Emulator to the CloudLab and Chameleon testbeds*, Inria, September 2016, n° RR-8955, https://hal.inria.fr/hal-01372050

Other Publications

[44] S. COOREVITS. *Fuzzing on the Openflow Protocol* , Telecom Nancy, September 2016, https://hal.inria.fr/hal-01386939

[45] J. FRANCOIS, A. LAHMADI, M. DAVIDS, G. M. MOURA. *IPv6 DOTS Signal Option*, October 2016, IETF DOTS - Internet Draft, https://hal.inria.fr/hal-01406267

[46] X. MARCHAL, T. CHOLEZ, O. FESTOR. *PIT matching from unregistered remote Faces: a critical NDN vulnerability*, ACM, September 2016, pp. 211 - 212, 3rd ACM Conference on Information-Centric Networking (ACM-ICN'16), Poster [*DOI :* 10.1145/2984356.2985224], https://hal.inria.fr/hal-01386809

[47] X. MARCHAL, M. EL AOUN, B. MATHIEU, W. MALLOULI, T. CHOLEZ, G. DOYEN, P. TRUONG, A. PLOIX, E. MONTES DE OCA. *A virtualized and monitored NDN infrastructure featuring a NDN/HTTP gateway*, ACM, September 2016, pp. 225 - 226, 3rd ACM Conference on Information-Centric Networking (ACM-ICN'16), Poster [*DOI :* 10.1145/2984356.2985238], https://hal.inria.fr/hal-01386615

[48] L. NUSSBAUM. *Usages et utilisateurs de Grid'5000: stratégie pour l'accès aux ressources*, March 2016, working paper or preprint, https://hal.inria.fr/hal-01294910

[49] W. M. SHBAIR, T. CHOLEZ, J. FRANÇOIS, I. CHRISMENT. *HTTPS Traffic Classification*, April 2016, Network Machine Learning Research Group (NMLRG), Internet Research Task Force (IRTF), Buenos Aires, Argentina, April 2016, https://hal.inria.fr/hal-01392838

References in notes

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

[51] N. FOSTER, A. GUHA, M. REITBLATT, A. STORY, M. J. FREEDMAN, N. PRAVEEN KATTA, C. MONSANTO, J. REICH, J. REXFORD, C. SCHLESINGER, D. WALKER, R. HARRISON. *Languages for software-defined networks*, in "IEEE Communications Magazine", 2013, vol. 51, n° 2, pp. 128-134

[52] 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