Journée des doctorants du département 3 (Réseaux, Systèmes et Services)
2018 PhD day of Department 3 (Networks, Systems and Services)

14/12/2018, room C005, LORIA

Program schedule

9:00 – 9:05 Welcome (Ye-Qiong Song)

9:05 – 10:30 session 1: Modeling, simulation and experimental methods

Béatrice Linot *(20' + 5' Q&A)*
Trust in Computer-Supported crisis management information sharing

Thomas Paris *(20' + 5' Q&A)*
Complex system modeling by composition

Abdulqawi Saif *(20' + 5' Q&A)*
Contributions of experimental methods for I/O systems and testbed experiments

Jean-Baptiste Wiart *(5')*
Definition of a domain specific language for the cosimulation of microgrid powered hydrogen

Théo Docquier *(5')*
Design, modeling and co-simulation of real-time industrial IoT for smart grids

---

10:30 – 10:50 coffee break

10:50 – 12:00 session 2: Internet of Things, SDN and security

Mingxiao Ma *(20' + 5' Q&A)*
Study of Synchronization Attacks on Distributed and Cooperative Control in Microgrid Systems

Grégoire Denis *(5')*
Malicious attacks detection and resilience in cyber-physical systems through joint dynamic resource scheduling and synthesis of adaptive control laws

Adrien Hemmer *(5')*
Predictive Security Monitoring for Large-Scale Internet-of-Things

Abir LARABA *(5')*
Data-Driven Intelligent Monitoring for Software-Defined Networks

Ahmad ABBOUD *(5')*

Compressed and Verifiable Filtering Rules in Software-defined Networking

Virgile Dauge *(20' + 5' Q&A)*
Systèmes Cyber-Physiques autonomes et communicants en milieux hostiles. Application à l'exploration par robots mobiles

---

12:00 – 12:30 Invited session

Prof. Enrico Natalizio *(25' + 5' Q&A)*
5G and UAVs: synergies to exploit for an Internet of Intelligent Things

---

12:30 – 14:00 Buffet & Discussion

14:00 – 15:15 session 3: Security

Hoang-Long Nguyen *(20' + 5' Q&A)*
Transparency Approach using Blockchain to End to End Encryption (E2EE)

Nicolas Schnepf *(20' + 5' Q&A)*
Orchestration and verification of security functions for smart environments

Victorien Elvinger *(20' + 5' Q&A)*
Prunable tamper-evident log in peer-to-peer systems

15:15 – 15:30 coffee break

15:30 – 17:10 session 4: Safety, Performance and Optimization

Louis Viard *(20' + 5' Q&A)*
Monitor-Centric Mission Definition For Cyber-Physical Systems

Quentin Laporte-Chabasse *(20' + 5' Q&A)*
A topological characterisation of peer-to-peer inter-organisational collaboration

Bilal Messaoudi *(20' + 5' Q&A)*
Multiple periods vehicle routing problems: a case study

Hoai-Le NGUYEN *(20' + 5' Q&A)*
Studying group performance and behavior in collaborative editing

---

Appendix: Abstracts of the presentations

(in order of the program schedule)

Session 1

Béatrice Linot

Trust in Computer-Supported crisis management information sharing

Abstract: My Doctoral research aims to identify the psychological and social factors that influence trust and determine the information sharing behavior of professional participants in the crisis response system. Building on the idea that the computer disrupts these factors, our aim is to design tools that restore the conditions of trust in a framework of collaborative information sharing. I combine theory and methods used in psychology and human factors, with computer science to determine how and why trust is degraded in relation to civil security operations. I propose to (1) identify the multi-level factors influencing trust during collaborative activities supported by computers (e.g., contextual factors, organizational factors, individual factors,); and (2) identify data-based design guidelines for digital devices that promote the sharing of information related to civil security and thereby develop and maintain shared situational awareness during collaborative activities.

Thomas Paris

Complex system modeling by composition

Abstract: Complex systems are systems composed of many heterogeneous interacting entities. For example, a smart-grid is a complex system which involves entities from at least three domains (power grid, telecommunication and information system). Multi-modeling (modeling each part of the system individually) and co-simulation (simulating each part separately and ensuring synchronization and data-exchange between simulators) are promising approaches to handle complexity but request to handle heterogeneities (domains, formalisms...).

MECSYCO (Multi-agent Environment for Complex System CO-simulation) is a co-simulation middleware with an integrative approach (reuse of legacy, pre-existing or even future systems) based on formal and software wrapping. It provides means to handle heterogeneities and to ensure modularity.

One of the challenges is to enable this integrative approach in a rigorous multi-modeling and co-simulation process while providing together the handling of heterogeneities, the modularity and the closure under coupling property (allowing hierarchical construct).

My PhD work consists in enhancing MECSYCO with a multi-modeling activity support and the closure under coupling property while maintaining its advantages. To meet this goal, we define dedicated description structures to manipulate the results of the three main steps of the multi-modeling and co-simulation process (integration, multi-modeling and experiment). The use of Domain Specific Languages is explored to guide this description activity. In parallel, several advances have been done on each step of the M&S process for MECSYCO. For example the integration of a multi-agent simulator or the design of complex coupling feature called multiplexers. These works open new perspectives concerning multi-model checking, co-simulation deployment...

Keywords: Modeling & Simulation, Composition, Complex System

Abdulqawi Saif

Contributions of experimental methods for I/O systems and testbed experiments

Abstract: In general, computer systems experimentation is a challenging activity as many experimental and environmental factors determine experiments flow. Focusing mainly on distributed storage systems, high-level evaluations are frequently used for studying I/O performance where fears that internal and low-level behaviors are not considered in these evaluations. Additionally, porting those experiments to developing environments like testbeds is not a trivial task. Many Challenges like customizing experiment resources based on the experiment needs, monitoring experiments activity via a reproducible method, and/or having a lightweight usage of testbed resources should be investigated.

In this thesis, we address those challenges by contributing experimental methods for both I/O systems, and monitoring & designing testbed experiments. We propose a low-level experimental method for revealing low-level I/O pattern-related issues in distributed storage system. Based on a tracing-based profiling mechanism, this method reduces the quantity of traces needed to be investigated. We then leverages the advantages of Cgroups (Linux control groups) to propose an /O emulation facility for customizing I/O experimental environments, building a suitable I/O environment over either homogeneous or heterogeneous resources. We then contribute to facilitate the experimentation activity on testbeds by proposing a monitoring framework for testbed experiments, eliminating the habitually ad hoc steps in experiment's data collection phase, so pushing towards experiments repeatability and reproducibility. We then optimize the design of greedy experiments via applying a statistical

method for limiting experiment's runs, guaranteeing to reach same experiment's conclusion with less resources' usage.
Keywords: Experimentation, I/O performance, tracing, experiment monitoring, experiment design

Jean-Baptiste Wiart

Definition of a domain specific language for the cosimulation of microgrid powered hydrogen

Abstract: Due to the energy transition, new production methods and energy consumption are emerging. This is the case of microgrids. These are micro smart grids, developed to respond quickly and automatically to specific situations such as power grid failures, natural disasters, power consumption peaks... However, developing and deploying such facilities is expensive. Simulation then became the means of studying such systems. These systems are however multi-source, and during modeling, it is necessary to describe the system as the integration of interacting heterogeneous sub-systems. Its simulation consists in managing the synchronization of heterogeneous simulators as well as the exchange of data between them. We speak about cosimulation. Tools have been developed, like Mecsyco, to address these problems. Nevertheless, it requires a lot of effort to acquire computer skills: whether it is the fact of programming or learning concepts such as the principles of formalism integration. My job is then to propose, develop software concepts and components, in particular DSL (Domain Specific Language) tailored for microgrid experts to bridge the gap between conceptual and multisource multi-carrier microgrid simulation.

Théo Docquier

Design, modeling and co-simulation of real-time industrial IoT for smart grids

Abstract: In this talk, we focus on the substation automation part of electric smart grids where data communication requires milliseconds order delay and full reliability guarantees. This arises challenging issues on the underlying Ethernet-based network architecture design, especially concerning its performance evaluation. In this talk, we present our study of the state-of-the-art solutions by introducing IEC 61850 standard and surveying on the performance evaluation of switched Ethernet for IEC 61850 substation automation. Both network calculus and simulation based state-of-the-art approaches are deeply analyzed and compared. Open issues are also discussed for identifying future research directions such as the need of in-depth traffic scheduling analysis, the potentials of introducing TSN into substation automation, and the co-simulation of both electric grid and communication network.

Session 2

Mingxiao Ma

Study of Synchronization Attacks on Distributed and Cooperative Control in Microgrid Systems

Abstract: Microgrids are adopted to provide distributed generation of renewable energy resources and scalable integration of loads. To ensure the reliability of their power system operations, distributed and cooperative control schemes are proposed by integrating communication networks at their control layers. However, the information exchanged at the communication channels is vulnerable to malicious attacks aiming to introduce voltage instability and blackouts. In our research, we design and evaluate a novel type of attacks on the cooperative control and communication layers in microgrids, where the attacker targets the communication links between distributed generators (DGs) and manipulates the reference voltage data exchanged by their controllers. We analyze the control-theoretic and detectability properties of this attack to assess its impact on reference voltage synchronization at the different control layers of a microgrid. Results from numerical simulation are presented to demonstrate this attack, and the maximum voltage deviation and inaccurate reference voltage synchronization it causes in the microgrid. We also build a hardware platform modeled after a simplified microgrid with DG units based on Raspberry Pi and Arduino boards, DC motors for power generation and light bulbs as electrical loads. We study the attacks using man-in-the-middle (MITM) and malware techniques to demonstrate and validate its impact on the microgrid synchronization and its voltage stability which affect end user's electrical devices.

Grégoire Denis

Malicious attacks detection and resilience in cyber-physical systems through joint dynamic resource scheduling and synthesis of adaptive control laws

Abstract: The goal is to counter denial-of-service attacks, as well as man-in-the-middle attacks that allow opponents to inject false data on control signals or on sensor-transmitted information to the facility via communication channels, and finally physical attacks on sensors and actuators close to defects. In this PhD thesis, to go beyond the current state of the art solutions, our original idea is to jointly design dynamic resource reallocation/scheduling and control law synthesis for drastically increasing the resilience of CPS face to malicious attacks. This can be achieved in SDN framework where physical plant controller and network controller may be merged. Simulations on SDN control operation were performed on Matlab. The purpose of this thesis is to apply what has been developed to a robot fleet: if one of the robots receives an attack, the robot fleet must be able to adapt.

Adrien Hemmer

Predictive Security Monitoring for Large-Scale Internet-of-Things

Abstract: Recently, Internet-of-Things has grow in importance in multiple domain such as domestic with smart-homes or industrial with the industry 4.0. It is complex to manage IoT infrastructure because each of its device can be really different, in addition they lack power and compute efficiency. Moreover, to add in complexity, the devices can be made by several third parties that do not use the same protocols for collecting or sending information. As a result, such a system is too complex to be absolutely secured, and is naturally a source of potential threats.

The objective of the thesis, in the context of the European H2020 project SecureIoT, to define and evaluate a predictive security framework for IoT for devices from multiple domains. The challenging goal is to observe evidences of future attacks or misuse by collecting and integrating heterogeneous data. In the new IoT architecture under construction, a security engine has to be designed for the predictive analysis. This engine has to perform a security assessment, using collected data, and support decision on counter-measures. However, the gathered data have to be meaningful in order to detect abnormal behaviours of systems. Furthermore, the monitoring and collection process have to be scalable to handle complex real-time ecosystem.

Abir LARABA

Data-Driven Intelligent Monitoring for Software-Defined Networks

Abstract: Monitoring is fundamental to infrastructure management. Accurate and timely statistics are essential for many management applications such as failure detection, load balancing, traffic engineering, accounting and intrusion detection. This must be achieved in a cost-effective manner, without introducing too much monitoring overhead. Network softwarization is creating opportunities for developing more effective monitoring solutions. For instance, the global network view available to SDN controllers facilitates the development of network monitoring applications that optimize monitoring frequencies and the placement of monitoring probes. A key research problem in network monitoring is to obtain accurate network monitoring data while incurring minimal monitoring overhead. In the research literature, several techniques have been proposed such as distributed monitoring. However, supporting online decisions in real-time with minimal overhead remains a challenge. In order to exploit the full potential of programmable networking hardware, the thesis will tackle the issue of accurate monitoring with minimal overhead through a data-plane approach. The goal is to monitor network with a minimal over-head and latency compared to dependent controller approach.

Ahmad ABBOUD

Compressed and Verifiable Filtering Rules in Software-defined Networking

Abstract: In this CIFRE PhD with the company NUMERYX, we are using a new filtering technique based on double-masked IP blocks for IP exact, prefix and arbitrary matching instead of using classical single masks. The multi-mask technique is able to aggregate IP blocks even not numerically adjacent and it helps compacting filtering policies and optimising the memory usage in networking devices. The goal of this PhD is to design, implement and evaluate multi-masked techniques for building a compressed and a verifiable filtering rules in Software Defined Networks with the possibility of distributing the workload processing among several packet filtering devices operating in parallel. The first axis of the work consists of designing efficient algorithms and models that can be implemented to compress the filtering lists in Software-defined Networks using the multi-mask compression techniques. The second axis of the work is dedicated to the formal verification of the resulting filtering rules and their consistence to detect and resolve conflicts, anomalies and non-compliance with the original filtering policies.

Virgile Dauge

Systèmes Cyber-Physiques autonomes et communicants en milieux hostiles. Application à l'exploration par robots mobiles

Abstract : Les systèmes cyber-physiques sont constitués par un ensemble d'éléments (agents) munis de capteurs et actionneurs, dotés de capacités de calcul et de communication, pouvant interagir avec l'environnement de manière coordonnée, mais pas obligatoirement centralisée. Dans ce sujet nous considérons des CPS qui peuvent être vus comme des systèmes multi-agents sûrs. Ces dernières années, les avancées dans le développement de ces systèmes a ouvert de nouvelles problématiques quant à la distribution et la gestion des calculs. En effet, l'intégration croissante des processeurs permet de disposer de ressources de calcul embarquées de plus en plus importantes (Nvidia Jetson TX1, carte parallela,...) et de capteurs plus complexes (Kinect, Intel realsense, camera stéréo HD Zed, Lidar 3D,...). Or, dès que les éléments d'un tel système ont des tâches un peu complexes à réaliser, comme par exemple de la reconstruction 3D ou de la prise de décision contextualisée la question de l'efficacité des calculs se pose. C'est tout particulièrement essentiel lorsqu'il y a des contraintes de réactivité des agents évoluant dans un environnement physique changeant et potentiellement hostile. Ainsi, il devient nécessaire de définir des stratégies de distribution et parallélisation des traitements à effectuer en fonction des capacités de calcul et de communication des agents et du contexte.

Les algorithmes de SLAM actuels utilisent différents mécanismes de calculs de transformations à partir de deux représentations (images, scans 3D) successives de l'environnement. Ces algorithmes sont souvent coûteux, et leurs résultats sont fortement dépendants de l'environnement. Il demandent également de déployer de nombreuses briques logicielles différentes dont le paramétrage influe sur la précision et la robustesse des résultats obtenus. Les tests que nous avons effectués avec des solutions "state of the art" se sont révélés décevants, tant en termes de précision que de robustesse.

Pour ces raisons, nous avons choisi de nous orienter vers une approche différente. Nous nous sommes inspirés des procédures des géomètres, utilisant des balises afin d'estimer leur position après un déplacement. Cette procédure peut être effectuée de manière autonome par une flottille de drones.

Nous sommes actuellement en cours de réalisation et de tests d'un système mobile, inspiré des systèmes statiques de motion capture. Les premiers tests sont encourageants, nous incitant à poursuivre nos travaux dans cette direction.

Invited Session

Pr. Enrico Natalizio (Invited speaker)

5G and UAVs: synergies to exploit for an Internet of Intelligent Things

Abstract: Cellular-connected UAVs and UAV-assisted 5G communications are the two main research and development directions individuated for UAVs usage in 5G. Cellular-connected UAVs, supported by recent standardization efforts for Long Term Evolution (LTE) systems, considers the UAVs as aerial users of the mobile network, whereas UAV-assisted 5G communications involves the usage of UAVs as a part of the infrastructure to improve the performance of the cellular system. However, the 5G communication paradigm proposes a new way of defining services, based on network functions virtualization and network slicing. Through these mechanisms, 5G consortia envisage the integration of million devices, towards a Massive Internet of Things. As UAVs are more powerful devices than classic IoT devices, in terms of self-organization, computation, storage, communication, reasoning, learning and moving capabilities, they could integrate with classic IoT devices into a cyberphysical system that provides the end-users with advanced services that exploit these capabilities. We argue that this integration is facilitated by leveraging 5G innovations, such as functions virtualization. In this talk, we first survey the two existing research and development directions, and then we propose to make a step forward in the integration of UAVs into larger IoT systems.

Session 3

Hoang-Long Nguyen

Transparency Approach using Blockchain to End to End Encryption (E2EE)

Abstract: My thesis focuses on improving E2EE to protect communication among users from different enterprises that maintain their own security servers. The system should protect communication over network from eavesdroppers, including ISPs, system providers and even the enterprises themselves while being scalable and easy to use. State of the art survey suggests the use of a key transparency system (e.g. Certificate Transparency, CONIKS) for such purpose. However, current approaches on key transparency mostly rely on a

separate gossiping protocol which is either, hard to implement, vulnerable to malicious clients or not scalable with a large number of users. We proposed 2 contributions throughout the thesis.
(1) We propose an auditing scheme using Ethereum blockchain to replace the gossip based audit protocol in state of the art system. Compare to related work, our proposal is easy to implement, inexpensive to operate and resilient to malicious clients.
(2) We conduct an empirical study on a theoretical attack on the use of blockchain in key transparency system (the eclipse attack). Based on the study results, we propose a light weight anomaly detection algorithm to detect such attack.

Nicolas Schnepf

Orchestration and verification of security functions for smart environments

Abstract: Security threats against smart environments are exponentially growing for several years due to lack of market preventive methods. A solution proposed by researchers consists in chaining security functions for dynamically protecting those devices: in particular, those chains would benefit of the programmability provided by software defined networks (SDN) for automating their deployment and their adjustment. Nevertheless, the multiplication and the complexity of such chains of security functions increase the risk of introducing misconfigurations in network policies: because of this complexity, the validation of such chains require the use of formal methods for guarantying their correctness before their deployment.
The goal of this PhD is to design a framework for the orchestration and the verification of chains of security functions. In our previous work we already designed an approach for the validation of security policy called synaptic: this framework relies on formal methods for validating the correctness of SDN policies. Complementary to this work we proposed an approach for automatically profiling android applications in order to identify their security requirements. The remaining part of our work will consist in designing an approach for automatically generating or selecting chains of security functions corresponding to the applications running on a device.

Victorien Elvinger

Prunable tamper-evident log in peer-to-peer systems

Abstract : In peer-to-peer collaborative systems, peers modify their own copy of a shared document. Because copies are concurrently modified, they diverge from each other. Peers eventually exchange and play every modification in order to get convergent copies. Convergence is a key property to ensure the success of a collaboration. Malicious peers can break convergence between honest peers by equivocating them. To protect convergence of copies, honest peers can maintain a replicated tamper-evident log. The log stores every modification of the document and makes equivocations evident. New peers have to retrieve the entire log in order to obtain the document and then to contribute. Thus, the cost of joining a collaboration increases with the size of this log. We propose that new peers retrieve an untrusted snapshot of the document and authenticate this snapshot using a pruned version of the log. Our main contribution lies in how to safely prune the log.
Keywords: Tamper-evident log; Authenticated log; Prunable log; Dyanmic group; Peer-to-peer systems; Convergence; Consistency; Causal Stability

---

Session 4

Louis Viard

Monitor-Centric Mission Definition For Cyber-Physical Systems

Abstract: Cyber-Physical Systems (CPS) have become ubiquitous. We entrust them with more and more features and autonomy, which magnifies the questions about their safety. CPS safety relies not only on the safety of their components but also on the mission they have to perform been well-defined. Ensuring such properties split up into two parts: static verification and run-time monitoring. The former leverages a model of the problem to assess the validity of a mission while the latter checks this model against the real world execution. To tackle the specification of correct missions, we propose a Domain-Specific Language. It is primarily thought to mitigate the consequences of the inevitable discrepancy between computable and real execution. To this effect, the language offers a dedicated structure to specify monitors and fallback behaviours. It fits into a toolchain (under development) featuring properties verification on a mission and automatic generation of executable code.

Quentin Laporte-Chabasse

A topological characterisation of peer-to-peer inter-organisational collaboration

Abstract : Decentralised collaborative applications emerged to address privacy, availability and security issues raised by the popular centralised collaborative platforms. Such applications lay on a peer-to-peer communication paradigm where each user is directly connected to the other involved collaborators. In that way, users individually keep control over their data. It might be required that several organisations (companies) have to work together to achieve challenges they cannot address individually. To preserve their sovereignty, involved organisations have to ensure that their sensitive information is never exposed. This requires controlling outgoing communications. At first sight, it sounds contradictory to comply with the federation's requirement while keeping peer-to-peer benefits. A proposal to deal with this tradeoff is to determine which peer-to-peer topology facilitate inter-organisational collaboration. This work consists of extracting topological features from real instances of inter-organisational collaborations. Exponential Random Graph Models appear to be a relevant class of models for social network analysis. They rely on realistic dependence assumptions and allow for better understanding of the social process behind tie creation. However, parameters estimation algorithms remain challenging and may cause degeneracy issue in some configurations. To overcome this problem, we propose to use the ABC Shadow algorithm, which improves the relevance of parameter estimation results. Ultimately, a well-estimated model enables a comprehensive characterisation of topological aspects of a peer-to-peer inter-organisational collaboration.

Keywords: Collaboration, P2P, Exponential Random Graph Model (ERGM), Markov Chain Monte Carlo (MCMC), Approximate Bayesian Computation (ABC)

Bilal Messaoudi

Multiple periods vehicle routing problems: a case study

Abstract: We consider a challenging problem faced by an hygiene services company. The problem consists of planning and routing a set of customers over a 3-months horizon period where multiple frequencies of visits can be required simultaneously by each single customer. The objective is then threefold: (1) balancing workload between vehicles (agents) (2) minimizing number of visits to the same customer (3) minimizing total routing costs. In this context, a routing plan must be prepared for the whole horizon, taking into account all constraints of the problem. We model the problem using a decomposition approach of planning horizon, namely, weeks planning and days planning optimization. We propose an adaptive large neighborhood search with several operators for routing phase of solving approach. To evaluate the performance of the solving approach we solve an industrial instance with more than 6000 customers and 69951 requests of visits. The results show an excellent performance of the solving approach in terms of solution quality comparing with the existing plan used by the hygiene services company.

Hoai-Le NGUYEN

Studying group performance and behavior in collaborative editing

Abstract: Collaborative editing (CE) allows a group of people to modify a shared document simultaneously (real-time) or non-simultaneously (asynchronous). It has gained in popularity with several free services and tools designed to support collaborative editing such as Google Drive, Wikipedia and Version control systems. Compared to asynchronous CE, in real-time CE, each collaborator receives immediately updates of other users and is therefore aware of the parts of the document being edited. However, when the number of collaborators increases, delays for seeing other users modifications are larger and conflicts still happen. Also, in real-time collaboration, performances are considered more important than in asynchronous collaboration. Collaboration traces collected from these systems represent a valuable data for research. We study group performance and behavior in CE by analyzing collaboration traces in both asynchronous and simultaneous contexts. In the first study, we analyzed the concurrency and conflicts in official Git repository of four projects: Rails, IkiWiki, Samba and Linux Kernel. We analyse the collaboration process of these projects at specific periods revealing how change integration and conflict rates vary during project development life-cycle. We also analyse how often users decide to rollback to previous document version when the integration process generates conflicts. In the second study, we analysed ShareLaTeX logs which were collected from a ShareLaTeX server used inside an Engineering school and anonymized for privacy purpose. The logs were conducted from collaborative editing of groups of three or four students which were assigned a writing task and required to use ShareLaTeX server hosted by the Engineering school. All editing activities were recorded by ShareLaTeX server from the beginning until the end of the assignment. In this study, we analyzed CE in both time and position dimension. Noted that in time dimension, two edits made by different users are considered as `simultaneous edits' if they are `closed enough' in time. So far the maximum `time gap' was chosen arbitrarily in previous related works.