Summer School on Cyber-Physical Systems 2013: some information

July 8-12, 2013
Grenoble, France

Organized by EIT ICT Labs and Persyval-Lab

http://persyval-lab.org/en/summer-school/cps

For any question, please contact us at:

cps-school.organization@imag.fr

About

Scientific Organization

EIT ICT Labs is one of the first Knowledge and Innovation Communities set up by the European Institute of Innovation and Technology, as an initiative of the European Union. EIT ICT Labs mission is to drive European leadership in ICT innovation for economic growth and quality of life.

PERSYVAL-Lab focuses on pervasive systems and algorithms at the convergence of physical and digital worlds. PERSYVAL-lab is built over high-level research laboratories present at Grenoble in Mathematics, Computer Science, Automatic Control, Signal Processing, and Hardware Architecture.

Domain

Cyber-Physical Systems (CPS) are engineered systems that are built from and depend upon the synergy of computational and physical components. CPS are becoming an important part of our daily life. Humans build, deploy, use, and maintain these systems that can sense our activities and influence our behavior. Examples of the many CPS application areas include the smart electric grid, smart transportation, smart buildings, smart medical technologies, next-generation air traffic management, and advanced manufacturing. CPS are expected to have great technical, economic and societal impacts in the near future.

CPS will transform the way people interact with engineered systems, just as the Internet transformed the way people interact with information. We will increasingly rely on these networked embedded systems, therefore also requiring a secure and privacy-preserving treatment of sensitive human-centric data. Novel paradigms and solutions are also needed to allow humans to interact with these systems. However, these goals cannot be achieved without rigorous systems engineering. Emerging CPS will be coordinated, distributed, and connected, and must be robust and responsive. The CPS of tomorrow will need to far exceed the systems of today in capability, adaptability, resiliency, safety, security, and usability.

The Summer School on Cyber-Physical Systems aims at bringing together researchers from industry and academia. This school explores the manifold relationship between networked embedded systems and humans as their creators, users, and subjects. The format of the Summer School will be a five-day meeting, organized around different aspects of rigorous systems engineering of Cyber-Physical Systems.

Goals

The goal of the summer school is to survey fundamental and applied aspects of CPS and their relationship to humans, as well as to identify novel opportunities and research directions in these areas through a series of lectures by international experts. Participants will also experience the relevant technologies during hands-on courses and be given a chance to present their own work. The school will provide a great opportunity to know other people working in the field, to meet distinguished scholars, and to establish contacts that may lead to research collaborations in the future.

Classes will range from basics of sensors to experience from real-world deployments, security, privacy, and dependability, debugging and validation of networked embedded systems, cyber-physical internet, online data Mining, virtual reality, rigorous CPS engineering, networked control systems, management and maintenance of networked embedded systems, interacting with networked embedded systems, applications such as smart energy and smart health-care.

Students participating at this summer school will learn the current state of the art in CPS and will be able to apply new techniques coming from various communities and backgrounds to their own domain. The CPS Summer School will be held at Grenoble University. Courses will be given in English by experts from industry and academia working in various fields of CPS.

Topics

- Computer security and cryptography.
- System modelling.
- Medical devices.
- Sensor networks.

Invited Speakers

- Prof. Jean-Claude Bajard - UPMC (France).
- Prof. Gilles Barthe - IMDEA Software Institute (Spain).
- Prof. Manfred Broy - TU Munich (Germany).
- Olivier Coutelou - Schneider Electric Grenoble (France).
- Prof. Alexandre David - Aalbord University (Denmark).
- Dr. Julien Francq - Cassidian (France).
- Prof. Yassine Lakhnech - Verimag (France).
- Prof. Kim G. Larsen - Aalborg University (Denmark).
- Dr. David Lesens - Astrium Space Transportation (France).
- Prof. Peter Marwedel - TU Dortmund (Germany).
- Prof. Doron Peled - Bar Ilan University (Israel).
- Prof. Pavithra Prabhakar - IMDEA Software Institute (Spain)
- Dr. Emmanuel Prouff - ANSSI (France).
- Prof. Oleg Sokolsky - University of Pennsylvania (USA).
- Prof. M. Törngren - KTH (Sweden).
- Dr. Jocelyne Troccaz - TIMC/CNRS, Grenoble (France).
- Dr. Thomas Watteyne - Dust Networks, Inc., Hayward (USA)

Scientific Board

- Prof. Manfred Broy (TUM, Mnchen).
- Prof. Joseph Sifakis (EPFL, Lausanne, and Verimag, Grenoble).
- Prof. Kim G. Larsen (Aalborg University).
- Prof. Marie-Christine Rousset (PERSYVAL-Lab and LIG, Grenoble).

Organization Committee

- Saddek Bensalem - University of Grenoble (France).
- Maria Victoria Cengarle - fortiss (Germany).
- Alessandro Cimatti - Fondazione Bruno Kessler (Italy).
- Nicolas Halbwachs - CNRS/Verimag (France).
- Martin Törngren - KTH Royal Institute of Technology (Sweden).
- Harald Ruess - fortiss (Germany).

Local Organization Committee

- Saddek Bensalem - University of Grenoble (France).
- Ylies Falcone - University of Grenoble (France).
- Nicolas Halbwachs - CNRS/Verimag (France).
- Erwan Jahier - CNRS/Verimag (France).

Important Dates

- School: **July 8-12, 2013**
- Social Event: **July 10, 2013**

Misc.

If you wish to have a certificate of participation to the school, please send an email with your contact information to `congress@floralis.fr`.

Venue

The school will be held in

> Institut Fourier
> 100 rue des mathématiques
> 38402 St Martin d'Hères cedex
> Grenoble Campus
> France

About Grenoble

Located in the southeastern part of France, Grenoble is considered as the capital of the Alps. Grenoble is surrounded by nature and high mountains: down the Alps, Grenoble is the meeting point of two important rivers, called "Drac" and "Isere". Grenoble has important historical and gastronomic heritages. Leisure activities in breathtaking nature are easily organizable and within short-distance. Grenoble is also a major scientific center in Europe dedicated to high-tech technologies, e.g., nano, micro, bio, and information technologies.

Hotel Information

On the school website you will find a list of hotels proposed by the Local Organizing committee.

Social Event

The social event of the school will take place on the 10th of July. Our social event will consist in a gastronomic banquet at Le Per'Gras, the best place to eat gastronomic food.

Le Per'Gras is located above La Bastille, Grenoble fortress. We will enjoy an outstanding view of the Alps with a gastronomic dinner.

To reach Le Per'Gras, we will take the cable car, the famous "Bubbles" of Grenoble. **The meeting point is the cable car station in Grenoble at 7:00pm.** *Please bring your badge to the social event, you will need it to get free access to the cable car.*

Please check the map on the school website.

The diner will start at 8pm.

Links:

– La Bastille: http://www.bastille-grenoble.fr/english/index.html
– Le Per'Gras: http://www.restaurant-grenoble-gras.com
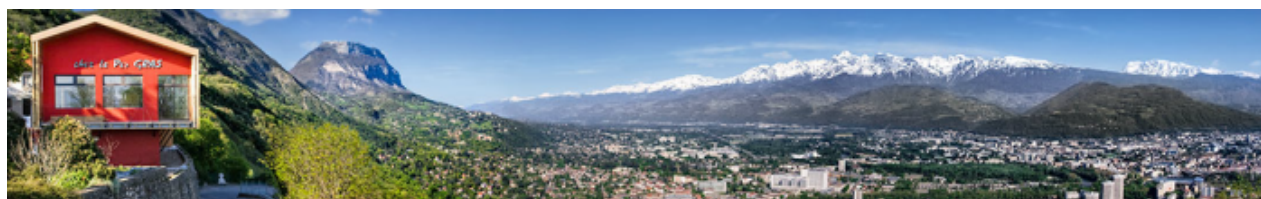
Program Overview

Time Slot	Monday 8th of July	Tuesday 9th of July	Wednesday 10th of July	Thursday 11th of July	Friday 12th of July
8:30 am - 9:00 am	WELCOME & OPENING				
9:00 am - 10:45 am	Prof. J-C. Bajard	Prof. M. Törngren	Prof. O. Sokolsky	Dr. T. Watteyne	Prof. M. Broy
10:45 am - 11:15 am	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break
11:15 am - 1:00 pm	Dr. E. Prouff	Prof. P. Marwedel	Dr. J. Troccaz	Dr. T. Watteyne (ctd)	Prof. K. Larsen
1:00 pm - 2:30 pm	Lunch	Lunch	Lunch	Lunch	Lunch
2:30 pm - 4:00 pm	Dr. J. Francq	Dr. D. Lesens	Prof. D. Peled	O. Coutelou	Prof. A. David
4:00 pm - 4:30 pm	Coffee Break	Coffee Break	Coffee Break	Coffee Break	Coffee Break
4:30 pm - 7:00 pm	Prof. Gilles Barthe Prof. Yassine Lakhnech & Student Session 1	Prof. P. Prabhakar (ends at 6pm)	Poster Session & Social Event	Student Session 2 (ends at 6pm)	Student Session 3 (ends at 6pm)

Talk Abstracts

Prof. Jean-Claude Bajard: Useful Arithmetic for Cryptography

Most of the asymetric cryptographic protocols are based on mathematical objects defined on finite fields (or finite rings). We present an overview of different representations and algorithms for fundamental operations like the modular multiplication. Some of them are particularly dedicated to hardware and embedded systems.

Prof. Gilles Barthe and Prof. Yassine Lakhnech: Computer-Aided Cryptographic Design and Analysis

Computer-aided cryptography aims to develop tools that support the design, analysis, and secure implementation of cryptographic constructions. In this presentation, I will give an overview of EasyCrypt (www.easycrypt.info), an interactive framework for building and verifying cryptographic proofs. I will outline its design principles, and then introduce the relational program verification technique which it uses to capture common patterns of reasoning in provable security. Finally, I will report on some recent developments to extend EasyCrypt to reason about cryptographic implementations in C, and to connect with the CompCert verified compiler to generate provably secure assembly code for cryptographic algorithms.

Prof. Manfred Broy: Modular Modeling Cyber Physical Systems

Abstract TBA.

Prof. Olivier Coutelou: Sensor Networks for industrial usage

Wireless sensors and sensor network becomes more and more important for Schneider Electric. After a short presentation of ZigBee Green Power, two examples will be described:

– Energy Monitoring of Machines in industrial factories.
– Energy and Electrical measurements dedicated to MV/LV substation in a Smart Grid environment.

At the end of the presentation, two real demos will be done:

– One to show simple self powered sensors allowing energy estimation.
– The other to demonstrate the capability of more complex sensors which are wirelessly synchronized in order to allow accurate electrical measurements.

Prof. Alexandre David and Prof. Kim Larsen: Symbolic and Statistical Model-Checking in UPPAAL.

In these two talks we will cover the theory of timed automata, our fundamental modeling language underlying the verification tool UPPAAL. Also, a number of extensions of this formalisms will be presented including timed games, priced timed automata and games, energy automata games, stochastic extensions of these as well as the most recently very expressive formalism of stochastic hybrid automata, which is particularly well-suited for modeling cyber-physical systems. We will review a number of associated decision problems related to model-checking, refinement checking and optimal scheduling and synthesis for these models that are highly relevant for cyber-physical systems.

The lectures will also emphasize the substantial research effort in the design of algorithms and datastructures for efficient analysis of timed automata and its extensions as to be found in the verification tool UPPAAL and its various branches. Also, substantial focus will be on the most recent statistical model checking engine of UPPAAL, where properties are settled up to user-specified level of confidence based on randomly generated simulation runs.

The lectures will include ample demonstration of UPPAAL and it extensions, in particular UPPAAL SMC, as well as applications to a range of real-time and cyber-physical examples including schedulability and performance evaluation of mixed criticality systems, modeling and analysis of biological systems, energy-aware wireless sensor networks, smart grid and energy aware buildings and battery scheduling.

Dr. Julien Francq: Hardware Trojans: Taxonomy and Detection Methods

Nowadays, for financial reasons, most of the Integrated Circuits (ICs) are designed, manufactured and tested in foreign countries. It is thus difficult to secure all the IC design flow: nothing can prevent from the insertion of any malicious and deliberate change to the IC (also called Hardware Trojans, HTs) that may cause unwanted effects and potentially damages in many sensitive applications (avionics, space, military devices, communication, industry, nuclear plants, etc.).

This presentation proposes first to show a taxonomy of the different HTs of the literature. We will see that this bestiary is very big. Then, we will detail the detection methods of the state-of-the-art with their limitations.

Destructive HT detection methods mainly consist in reverse-engineering ICs before deployment, which is very costly and does not guarantee 100% detection rate. Moreover, non-destructive HT detection methods (logic test, side-channel analysis, etc.) have also to face challenges (process variation noise, measurement noise, low controllability and observability of nodes, etc.). Finally, the speaker will show the French funded R&D project HOMERE (Hardware Trojans: Threats and Robustness of Integrated Circuits), which will try to progress beyond the state-of-the-art.

Dr. David Lesens: Modelling in an industrial context

Model Driven Engineering is the topic of numerous theoretical research projects. But what about its real use in the industry? The objective of this talk is to provide some elements of answer for the space domain. Several topics will be addressed:

– Objectives of modelling,

- Expected benefits / risks,
- Perimeter of modelling (system, software, hardware, mechanical...),
- Needs of guidelines,
- Training of development teams,
- Language's semantics,
- Automatic code generation.

These topics will be supported by feedbacks from operational uses.

Prof. Peter Marwedel: Efficient Computing in Cyber-Physical Systems

Computing in cyber-physical systems has to reflect the context of the computations and, hence, has to be efficient in terms of a number of objectives. In particular, computing has to be (worst and average case) execution-time and energy efficient, while also being reliable. In this talk, we will consider optimization techniques targeting worst-case execution time (WCET) and energy efficiency.

In the first part, we will consider real-time constraints and WCETs. We do this by integrating compilers and WCET estimation. We will demonstrate how such integration opens the door to WCET-reduction algorithms. For example, an algorithm for mapping frequently accessed memory objects to scratch pad memories (SPMs) is able to reduce the WCET for an automotive application by about 50%. The need to seriously consider WCETs and time constraints also has an impact on applicable error correction techniques. We will demonstrate our approach for a flexible error handling in the presence of real-time constraints possibly prohibiting time consuming error corrections.

In the talk, we will also address the energy consumption of computing in cyber-physical systems. We will explain how scratch pad memories can be used to reduce the energy consumption of such systems. Also, we will demonstrate that graphic processing units (GPUs) provide another way of saving energy. The talk will finish with some remarks on cyber-physical system education.

Prof. Doron Peled: Components based systems with probabilities

In the design of reliable complicated systems, one can benefit from a high level formalism that is close enough to the specification, and, on the other hand, automatically and efficiently translatable into the physical layer. Component-based systems can represent a collection of units working together, with an emphasis on the interactions, choices and concurrency among their actions. Adding the ability of making probabilistic choices in component-based systems is nontrivial since each component has its own view, which is partial to the global view of the entire system; maintaining a global view would just eliminate the concurrency. A solution for that is to precede each probabilistic choice by a phase where the local view of a component is locked in order to prepare for such a decision. In this lecture, I would present the mathematical concepts related to concurrent probabilistic systems, based on Markov Decision Processes. Then, a solution based on concurrent artifacts such as independence and confusion will be given. A simple and elegant implementation of component-based systems with probabilistic choices, using semaphores, will be described.

Prof. Pavithra Prabhakar: Formal Verification of Cyber-Physical Systems

The ubiquitous deployment of cyber-physical systems in safety critical applications such as aeronautics, automotive, medical devices, industrial process control and others, has pressurized the need for the development of automated analysis methods to aid the design of high-confidence systems. The lecture will focus on the application of formal methods for the verification of cyber-physical systems.

The focus of the lecture will be on the interaction of the discrete and the continuous dynamics exhibited by cyber-physical systems due to the interaction between a network of embedded processors and a physical world. Systems exhibiting mixed discrete-continuous behaviors are popularly referred to as hybrid systems. An overview of the state-of-the-art in hybrid systems verification will be provided. This will include an introduction to:

1. Formal models of hybrid systems.
2. Safety and stability properties.
3. Computational difficulty of the analysis.
4. Approximation algorithms.
5. Software tools.

Dr. Emmanuel Prouff: Side Channel Analysis Based on Linear Regression: From Paper to Silicium

Since the preliminary works of Kocher et al. in the nineties, studying and enforcing the resistance of cryptographic implementations against Side Channel Analysis (SCA) is became a dynamic and prolific area of embedded security. Stochastic attacks, introduced by Schindler et al. at CHES 2005, form one of the main families of SCA and they offer a valuable alternative to template attacks which are known to be among the most efficient ones. However, stochastic attacks, as long as template attacks, have been initially designed for adversaries with a perfect copy of the target device in hand. Such a prerequisite makes them a pertinent tool when studying the implementations resistance against the most powerful adversaries, but it limits their pertinence as a cryptanalytic technique. Indeed, getting open access to a copy of the device under attack is difficult in practice and, even when possible, it remains difficult to exploit templates acquired on one device to attack another one. In light of this observation, several papers have been published to adapt stochastic attacks for contexts where the above prerequisite is no longer needed. They succeeded in defining practical attacks against unprotected implementations but no work was published until now to explain how stochastic attacks can be applied against secure implementations. The proposed presentation aims at dealing with this issue. I will first show haw to extend the previous analyses of stochastic attacks to highlight their core foundations. Then, I will explain how they can be generalized to defeat first-order masking techniques, which are the main SCA countermeasures. Eventually, I will illustrate the interest of the new attack by a series of experiments on simulated and real electro-magnetic measurement traces.

Prof. Oleg Sokolsky: Challenges in Medical CPS

Modern techniques for treating patients are very dependent on medical devices. Medical devices include sensors, which provide vital information about patient state; actuators that effect treatment; and decision support systems that help clinical personnel in planning the treatment. Increasingly, devices used in treating a patient are interconnected, forming a patient-centric cyber-physical system (CPS). Medical CPS hold out the promise of improved patient care with fewer opportunities for human error and decreased treatment costs. In particular, medical CPS enable the development of physiologically closed-loop approaches that automatically deploy safety measures in response to changes in the patient's condition. At the same time, deployment of such medical CPS presents a variety of challenges. This lecture will discuss design, deployment, and regulatory challenges and suggest possible ways to overcome then, motivated by several on-going projects at the University of Pennsylvania. We will start with safety considerations for individual devices, such as infusion pumps and pacemakers; explore the implications of interoperability in collections of medical devices used in a treatment of a patient; and finally consider some of the clinical applications that are enabled by interconnecting medical devices.

Prof. Martin Törngren: Integrating Viewpoints in the Development of CPS

The development of CPS involves multiple stakeholders which have different viewpoints and therefore use different concepts, models and tools to deal with their concerns of interest. Successful development requires that relations between viewpoints are addressed. This lecture identifies that such relations exist at three levels: people, models and tools. We present solutions that formally and explicitly capture these relations at each of these three levels. Interrelation contracts are used to define the vocabulary, assumptions and constraints required for ensuring smooth communication between stakeholders (people level). Dependency models capture relations between product properties belonging to different viewpoints, and how such dependencies relate to predictions and decisions (model level). Tool integration models describe the relations between tools in terms of traceability, data exchange, invocation and notifications (tool level). An industrial robot case study is utilized to illustrate the challenges and solutions with respect to relations between viewpoints. We also provide an unification approach discussing how these solutions complement and can be used to support each-other.

Prof. Jocelyne Troccaz: Medical CyberPhysical Systems in use: the example of Computer-Assisted Medical Interventions

Computer-Assisted Medical Intervention systems aim at providing assistance to clinicians for planning, simulating and executing safely, accurately and efficiently diagnostic or therapeutic actions. Such systems

are based on a strong connection between digital data (patient images and signals, a priori information embedded in atlases, statistical models, biomechanical models, surgical protocols, etc.) and the real world where the clinician has to operate the patient. Collections of sensors may enable intra-operative data acquisition for refined decision making and action monitoring; actuators such as robots may be involved in the action itself with different levels of cooperation with a human operator. CAMI systems raise typical issues of CPS related to autonomy, security or dependability. In order to illustrate how these issues can be tackled in real applications, we will introduce the domain of CAMI and we will describe several examples from clinical end-user specifications to scientific and technological solutions we implemented.

Prof. Thomas Watteyne: Standardizing the Internet of (Important) Things: IEEE802.15.4e Low-Power Mesh Technology and 6TSCH.

The Internet of Things revolution is at our doorstep and with it an epochal turnpoint in wireless network design. Major standardization bodies work on low-power wireless mesh networks, how they can operate reliably (WirelessHART, IEEE802.15.4e, IETF RPL) and how they integrate within the Internet (IETF 6LoWPAN, CoAP). This talk will highlight the challenges faced by low-power wireless mesh networks, before showing how communication protocols and standards can address these. Numerous use cases, examples and lessons learnt will be taken from open-source and commercial implementations, as well as from the recent work at the IETF 6TSCH group.

Student Session 1 (Monday 8th of July, starts at 5:30pm)

Anthony Dessiatnikoff: Exploiting low-level vulnerabilities in avionics computing systems

The critical real-time embedded systems as avionics systems are more and more subjects to security issues. These systems are especially vulnerable due to the increasing complexity of the applications, the connectivity of the systems between un-controlled networks, the use of COTS and the resources sharing between applications. To solve these problems, some methods can be used: formal methods, security mechanisms and tools, vulnerabilities analysis and countermeasures. We focus our work on the last method. In this presentation, we will talk about the possible security weaknesses and the countermeasures in avionics systems.

Abdelberi Chaabane: You are what you like! Information leakage through users' Interests

Suppose that a Facebook user, whose age is hidden or missing, likes Britney Spears. Can you guess his/her age? Knowing that most Britney fans are teenagers, it is fairly easy for humans to answer this question. Interests (or "likes") of users is one of the highly-available on-line information. In this paper, we show how these seemingly harmless interests (e.g., music interests) can leak privacy-sensitive information about users. In particular, we infer their undisclosed (private) attributes using the public attributes of other users sharing similar interests. In order to compare user-defined interest names, we extract their semantics using an ontologized version of Wikipedia and measure their similarity by applying a statistical learning method. Besides self-declared interests in music, our technique does not rely on any further information about users such as friend relationships or group belongings. Our experiments, based on more than 104K public profiles collected from Facebook and more than 2000 private profiles provided by volunteers, show that our inference technique efficiently predicts attributes that are very often hidden by users. To the best of our knowledge, this is the first time that user interests are used for profiling, and more generally, semantics-driven inference of private data is addressed.

Guenaelle De Julis, Kevin Layat, Mathilde Soucarros: The problematic of random bit generators for cyber-physical systems

RBGs (Random Bit Generator) play a critical role in cybersystems, and particularly those providing security services. A consequence is that it is necessary to have a high level of confidence in them. In this work, we tested different RBGs while attacking them. We showed that the behavior of these RBGs can be modified. Recently, there has been an increased effort towards the standardization of RBGs in

certification schemes. The aim is to ensure the correct functioning of RBGs by implementing mechanisms preventing or informing of any undesired event. A current way to increase confidence in RBGs is to evaluate the randomness by applying several statistical tests. The reliability of their results depends on the estimated model of the RBG and the chosen methodology. The main batteries (Knuth, DieHard, NIST, AIS31, testU01) are only able to test one particular model and the binary answer cannot bring us information about the right model. We need to highlight local anomalies and more likely model with a deeper analysis. The search for the right model is also a problem when we measure the entropy produced by the RBG : several formulae are possible according to the model. Thus, we have to define and use an entropy estimator which will not overestimate the real entropy whatever could be the model.

As a consequence we need to define a better modeling of RBGs in order to improve interpretations of statistical tests and increase robustness against perturbations. To do so we have to study physical sources such as jitter, metastability in electronics or radioactive decay. The idea is to take into consideration specificities of the different sources in the interest of computing probabilities like the probability of bit appearance or pattern appearance. These probabilities would be adapted to the physical model and so the test derived from would be more pertinent.

Student Session 2 (Thursday 11th of July, starts at 4:30pm)

Roudy Dagher: On the usage of WSN for navigating in Smart Cities of the future

Sailors first navigated close to the shore by sighting landmarks. For traveling across the oceans, processes such as Dead Reckoning and celestial navigation had to be invented. In the 20th century, ground-based radio navigation systems were introduced. And in the late seventies, the GPS, a satellite radio navigation system was introduced for military applications and then opened for civilians.

GPS-based applications, especially in smart-phones, have changed our daily lives. We can navigate (almost) anywhere, with the assurance to reach our final destination. With the emergence of Smart City concept, Wireless Sensor Networks (WSNs) have become one of the key technologies for instrumenting the city, and thus providing its inhabitants with various services meant to improve their daily life. One of the identified applications is Smart Street Lightning, where the lamps are in a mesh network for remote control (energy saving) and maintenance purposes.

After a brief review of GPS technology, this talk introduces Ubiquitous Navigation System (UNS), a WSN-based navigation system, which takes benefit from the Smart Street Lightning system to provide a local navigation service.

Miriam Garcia Soto: Stability analysis of Hybrid Systems

This talk introduces a novel abstraction technique and a model checking algorithm for analysing stability of a particular class of hybrid systems. Hybrid systems are physical systems evolving in time, which exhibit a mixed discrete and continuous behaviour. Such an interaction is an inherent aspect of CPS. Stability is a control design property establishing that small perturbations on the input just induce small changes on the output.

The proposed technique consists of defining a simple system, an abstraction, from an initial hybrid system, and applying a model checking algorithm to determine stability. The proposed abstraction procedure is a modified predicate abstraction, which gives an abstract weighted graph. Model checking consists of analysing the finite weighted graph for the absence of certain kinds of cycles which can be solved by dynamic programming. It is shown that the abstraction is sound in that a positive result on the analysis of the graph implies that the original system is stable.

The feasibility of the approach has been demonstrated by a prototype implementation.

This is a joint work with Pavithra Prabhakar.

Ibrahim Amadou: On the efficiency of CSMA-based backoff algorithms for channel Reservation in RFID system

Mitigating reader-to-reader collisions is one of the principal challenges in a large-scale dynamic RFID system with a number of readers deployed in order to maximize the system performance (i.e., throughput,

fairness and latency). In prior works, contention-based and activity scheduling medium access control (MAC) protocols are commonly used approaches to reduce such problems. Existing protocols typically perform worse in a large-scale RFID dynamic system and require more additional components or are based on unrealistic assumptions. So far, many research efforts have been made to improve the performance or the reliability of Carrier Sense Multiple Access (CSMA) techniques for Mobile Ad-Hoc Networks (MANETs) by using an adaptive Backoff schemes. In this paper, we look at these well known solutions that proved their efficiency in high congestion wireless networks. We evaluate the performance and characterize these solutions when they are used to reserve the wireless channel through broadcasting message for reader-to-tag communication. Based on the application requirements, we study their capacity to mitigate collisions, the channel access latency, the average number of successful requests sent per reader and the fairness index in the context of RFID networks.

Milan Erdelj, Tahiri Razafindralambo, David Simplot-Ryl: Mobile robot deployment in the context of WSN

In this talk, a distributed algorithm for Point of Interest (PoI) coverage with mobile wireless sensors is presented. The goal of the algorithm is to cover the PoI with a set of sensors while maintaining the connectivity with a fixed base station. The algorithm is distributed, needs only local information at each sensor, does not require synchronization and is divided into three parts. In the first part, the sensor computes its future movement direction depending on its actual location and the location of PoI. In the second part, the distance that has to be covered by the sensor and its speed is computed. The third part is devoted to sensors motion. Unlike other algorithms described in the literature, our algorithm maintains the connectivity all along the deployment procedure and therefore allows the tracking of mobile PoI. The connectivity maintenance of our algorithm is done by using the properties of the Relative Neighborhood Graph (RNG). Indeed, if a graph G is connected, the Relative Neighborhood Graph extracted from G is also connected. Hence, during their movements, the sensors have only to keep the connection with their RNG neighbors to keep the whole graph connected. Moreover, the computation of the RNG uses only local information. We evaluate the performance of the proposed algorithm regarding the number of sensors that cover the PoI, the deployment speed and the energy consumption. Furthermore, we provide some results regarding the coverage of moving PoI and multiple PoIs. Finally, we implement our algorithm on Wifibot mobile robots and show that our algorithm can be easily implemented and can work in real conditions by using a simple collision avoidance scheme.

Student Session 3 (Friday 12th of July, starts at 4:30pm)

Alexandr Murahkin and Zubair Akhtar: Architecture modeling with variability and uncertainty

Traditional approaches of architectural modeling assume fully specified selection of components. We are currently exploring modeling with variability and uncertainty in the context of architecture modeling. The work involves creating the metamodel of AADL constructs in Clafer (a modeling language), and using that metamodel to create architectural models. The major advantage of this work is using the capabilities of Clafer on AADL models for expressing variability and uncertainty. Clafer Instance Generator & Optimizer will allow us to support design explorations of architectural models also in the presence of variability. Due to the limitations of Clafer, current challenges include tool scalability to support elaborate models, compilation time and complication in modelling of some of the AADL constructs. Moreover, since Clafer does not support behavioral modelling, only the structural aspects of the an model are being considered for now.

Michele Lora: Modeling and Verification techniques for Cyber-Physical Systems design

The heterogeneity to Cyber-Physical Systems is nowadays tackled mainly by employing top-down approaches, often based on the concept of model-based design. Bottom-up approaches are limited to using cosimulation, which does not provide any formal assurance about the correctness of the integration.

In this talk UniverCM will be introduced. UniverCM is an automaton-based formalism that allows to model both analog and discrete behaviors, together with typical SW behaviors. The major advantage of

this MoC is the possibility to map heterogenous systems into it and to represent them in a homogeneous environment allowing to easily integrate components coming from different domains. For these reasons, UniverCM is presented as the core representation used to develop a set of methodologies for highly heterogenous Cyber-Physical Systems design, by extending methodologies developed for homogeneous, purely digital, embedded systems.

Mengxuan Zhao: Supervisory controller for physical entities in Internet of Things and Smart Environments

New application domains of control, such as in the Internet of Things (IoT) and Smart Environments, require recourse generic control rules enabling the systematization and the automation of the controller synthesis. This work presents a generic architecture with supervisory controller as a service, as well as an automatic mechanism of synthesis of discrete controllers, in order to coordinate physical entities of various nature to respect generic control objectives in the Internet of Things and Smart Environments.