IDEA4CPS Workshop, Aalborg September 25-26

Venue: Restaurant Skovbakken inside Aalborg Zoo, Mølleparkvej 63, 9000 Aalborg

25 September:

9:00 – 9:30 Welcome and Coffee

9:30 – 11:00

Roberto Vigo: Trust-based Enforcement of Security Policies (30 min)

Bingtian Xue: Adequacy and Complete Axiomatization for Timed Modal Logic (30 min)

Hanne Riis Nielson: Disjunctive Information Flow (30 min)

11:00 – 11:30 Coffee break

11:30 – 12:30

Radu Mardare: The landscape of the Markov processes realm (30 min)

Giorgio Bacci: On the total variation distance of semi-Markov processes (30 min)

12:30 – 14:00 Lunch Break - Restaurant Skovbakken

14:00 – 15:30

Manfred Jaeger: Continuity Properties of Distances for Markov Processes (30 min)

Erisa Karafili: Energy Saving by Ambient Intelligence Techniques (30 min)

Giovanni Bacci: Computing Bisimilarity Distances over Continuous-time Markov Chains (30 min)

15:30 – 16:00 Coffee Break

16:00 – 17:00

Zaruhi Aslanyan: Pareto Efficient Solutions of Attack Trees (30 min)

Phan Anh Dung : Z3Opt: An optimizing SMT solver (30 min)

Phan Anh Dung : Z3Opt: An optimizing SMT solver (30 min)

18:30 – 22:15 Social Dinner – Restaurant Duus Vinkælder, Østerågade 9, 9000 Aalborg

26 September:

9:00 – 10:30

Jiri Srba: A Forward Reachability Algorithm for Bounded Timed-Arc Petri Nets (30 min)

Alberto Lluch Lafuente: A semiring-valued temporal logic (30 min)

Alessandro Bruni: Set-based abstractions in the applied π-calculus (30 min)

10:30 – 11:00 Coffee break

11:00 – 12:00

Yue Zhang : Energy-efficient fault management of WSNs (30 min)

Sebastian Alexander Mödersheim : Sufficient Conditions for Vertical Composition of Security Protocols (30 min)

12:00 – 13:30 Lunch Break - Restaurant Skovbakken

13:30 – 15:30

Peter Jensen: Memory Efficient Data Structures for Explicit Verification of Timed Systems (30 min)

Jakob Taankvist: On Time with Minimal Expected Cost! (30 min)

Danny Bøgsted Poulsen: Quantified Dynamic Metric Temporal Logic for Dynamic Networks of Stochastic Hybrid Automata (30 min)

Zhengkui Zhang: Verification and Performance Evaluation of Timed Game Strategies (30 min)

Abstracts

Roberto Vigo: Trust-based Enforcement of Security Policies,
joint work with A. Celestini, F. Tiezzi, R. De Nicola, F. Nielson, H. Riis Nielson

Two conflicting high-level goals govern the enforcement of security policies, abridged in the phrase "high security at a low cost". While these drivers seem irreconcilable, formal modelling languages and automated verification techniques can facilitate the task of finding the right balance. We propose a modelling language and a framework in which security checks can be relaxed or strengthened to save resources or increase protection, on the basis of trust relationships among communicating parties. Such relationships are automatically derived through a reputation system, hence adapt dynamically to the observed behaviour of the parties and are not fixed a priori. In order to evaluate the impact of the approach, we encode our modelling language in StoKlaim, which enables verification via the dedicated statistical model checker SAM. The overall approach is applied to a fragment of a Wireless Sensor Network, where there is a clear tension between devices with limited resources and the cost for securing the communication.

Bingtian Xue: Adequacy and Complete Axiomatization for Timed Modal Logic
Joint work with S. Jaziri, K.G.Larsen, R.Mardare

We develop the metatheory for Timed Modal Logic (TML), which is the modal logic used for the analysis of timed transition systems (TTSs). We solve a series of long-standing open problems related to TML. Firstly, we prove that TML enjoys the Hennessy-Milner property and solve one of the open questions in the field. Secondly, we prove that the set of validities are not recursively enumerable. Nevertheless, we develop a strongly-complete proof system for TML. Since the logic is not compact, the proof system contains infinitary rules, but only with countable sets of instances. Thus, we can involve topological results regarding Stone spaces, such as the Rasiowa-Sikorski lemma, to complete the proofs.

Hanne Riis Nielson: Disjunctive Information Flow
joint work with Flemming Nielson and Ximeng Li

Information flow aims at ensuring that confidentiality and integrity are maintained as data is being manipulated by programs. We study the challenge of achieving this when the information flow policies depend on actual data values — as in the case of a multiplexer combining and subsequently splitting data from different sources with different policies.
A main element of our solution is a semantic interpretation of information flow policies that makes clear the opposite direction of flow between confidentiality and integrity constraints. Another main element is the integration of a type system for confidentiality and integrity constraints with a Hoare logic for tracking data values.

Radu Mardare: The landscape of the Markov processes realm
Joint work with D. Kozen, P. Panangaden and K. Larsen

We describe the mathematical landscape where Markov processes live. This will synthetize results that we obtain in the last years in the attempt of providing a comprehensive understanding of the concept of

Markov process, its relation with logics and probabilistic bisimulation as well as with the bisimilarity distances.

Giorgio Bacci: On the total variation distance of semi-Markov processes
Joint work with Giovanni Bacci, K.G. Larsen and R. Mardare

We study the total variation distance between semi-Markov processes with emphasis on its relation wrt to the model checking problem of real-time specification expressed either as Metric Temporal Logic (MTL) formulas or timed languages recognized by Timed Automata (TAs). In addition we develop a general theory of approximation of the total variation distance both considering its algorithmic and expressivity aspects.

Manfred Jaeger: Continuity Properties of Distances for Markov Processes
Joint work with K.G. Larsen, H. Mao, R. Mardare

We investigate distance functions on finite state Markov processes that measure the behavioural similarity of non-bisimilar processes. We consider both probabilistic bisimilarity metrics, and trace-based distances derived from standard Lp and Kullback-Leibler distances. Two desirable continuity properties for such distances are identified. We then establish a number of results that show that these two properties are in conflict, and not simultaneously fulfilled by any of our candidate natural distance functions. An impossibility result is derived that explains to some extent the fundamental difficulty we encounter.

Erisa Karafili: Energy Saving by Ambient Intelligence Techniques

Nowadays the problem of energy consumption is becoming a pressing problem. We present an innovative system named Elettra able to allow people to monitor and control energy consumption in one or more buildings. For improving Elettra we introduce different methods taken from ambient intelligence. Through these methods we can infer energy consumption, construct a plan for decreasing energy consumption, improve this plan and adopt it to the system. The implementation of these methods to Elettra helps its automation and increases its efficiency.

Giovanni Bacci: Computing Bisimilarity Distances over Continuous-time Markov Chains
Joint work with Giorgio Bacci, K.G. Larsen and R. Mardare

We describe recent work on a bisimilarity distance between continuous-time Markov chains (CTMCs) and study the problem of computing it by comparing three different techniques: iterative, linear program, and on-the-fly.

Zaruhi Aslanyan: Pareto Efficient Solutions of Attack Trees
joint work with F. Nielson

Attack trees are widely used to model security threats of organisations and represent attack scenarios in an intuitive manner. Standard attack trees combine subtrees either conjunctively or disjunctively, thereby limiting their expressiveness. Moreover, in multi-parameter models, values characterising basic

attacks are propagating to the root relying on local decision strategies. In case of incomparable values, this approach may yield sup-optimal results.
To overcome these limitations, we extend the attack tree model with negation and devise automated techniques that quantify attack scenarios with sets of Pareto optimal solutions in the case of multiple objectives. We illustrate the development on a home-payment system.

Jakob Taankvist: On Time with Minimal Expected Cost!

Classical synthesis techniques solve (priced timed) games ensuring safety, or cost-bounded reachability objectives despite worst-case behaviors of an adversary. Assuming a stochastic environment, we can view these games as infinite-state Markov decision processes and it is possible to find strategies for reachability objectives minimizing some expected cost, though without guarantees. In this paper, we provide efficient methods for computing strategies that both ensure cost-bounded reachability objectives and provide (near-) optimal expected cost. Our method extends the synthesis algorithm of Uppaal-Tiga with a reinforcement learning technique that exhibits several orders of magnitude improvements w.r.t. previously known automated methods.

Jiri Srba: A Forward Reachability Algorithm for Bounded Timed-Arc Petri Nets

Timed-arc Petri nets (TAPN) are a well-known time extension of the Petri net model and several translations to networks of timed automata have been proposed for this model. We present a direct, DBM-based algorithm for forward reachability analysis of bounded TAPNs extended with transport arcs, inhibitor arcs and age invariants. We also give a complete proof of its correctness, including reduction techniques based on symmetries and extrapolation. Finally, we augment the algorithm with a novel state-spacereduction technique introducing a monotonic ordering on markings and prove its soundness even in the presence of monotonicity-breaking features like age invariants and inhibitor arcs. We implement the algorithm within the model-checkerTAPAAL and the experimental results document an encouraging performance compared to verification approaches that translate TAPN models to UPPAAL timed automata.

Alberto Lluch Lafuente: A semiring-valued temporal logic

I would like to present a semiring-valued temporal logic that we developed some years ago and to discuss its relations with respect to some recent developments in the area of quantitative verification. The logic is essentially a generalisation of CTL interpreted over constraint semirings, an algebraic structure that is quite suitable to model quantitative aspects such as quality-of-service measures. I will briefly mention some applications and results, and I will try to establish some connection with models and logics developed in recent years.

Alessandro Bruni: Set-based abstractions in the applied π-calculus
Joint work with Sebastian Mödersheim, Flemming Nielson, Hanne Riis Nielson

Many real world security protocols require a certain amount of state for different reasons: encryption keys need to be updated periodically to prevent attackers from learning valid ones, messages are signed with timestamps in order to avoid replaying them after they are no longer valid, etc. Specialised

protocols that need to run with bandwidth and real-time constraints may rely solely on state mechanisms to provide their claimed security properties, such as MaCAN and CANAuth, two proposed protocols for automotive that we recently analysed.
We propose an extension of the applied π-calculus with support for potentially infinite sets of values. With this extension we are able to analyse protocols with unbounded number of sessions, where security and authenticity properties rely on the use of counters and timestamps, or databases of keys.

Peter Jensen: Memory Efficient Data Structures for Explicit Verification of Timed Systems

Timed analysis of real-time systems can be performed using continuous (symbolic) or discrete (explicit) techniques. The explicit state-space exploration can be considerably faster for models with moderately small constants, however, at the expense of high memory consumption. In the setting of timed-arc Petri nets, we explore new data structures for lowering the used memory: PTries for efficient storing of configurations and time darts for semi-symbolic description of the state-space. Both methods are implemented as a part of the tool TAPAAL and the experiments document at least one order of magnitude of memory savings while preserving comparable verification times.

Sebastian Alexander Mödersheim : Sufficient Conditions for Vertical Composition of Security Protocols
joint work with Luca Vigano'

Vertical composition of security protocols means that an application protocol (e.g., a banking service) runs over a channel established by another protocol (e.g., a secure channel provided by TLS). This naturally gives rise to a compositionality question: given a secure protocol P_1 that provides a certain kind of channel as a goal and another secure protocol P_2 that assumes this kind of channel, can we then derive that their vertical composition $P_2[P_1]$ is secure? It is well known that protocol composition can lead to attacks even when the individual protocols are all secure in isolation. In this paper, we formalize seven easy-to-check static conditions that support a large class of channels and applications and that we prove to be sufficient for vertical security protocol composition.

Yue Zhang : Energy-efficient fault management of WSNs

Danny Bøgsted Poulsen: Quantified Dynamic Metric Temporal Logic for Dynamic Networks of Stochastic Hybrid Automata
joint work with Alexandre David, Kim G. Larsen, Axel Legay and Guangyuan Li

Multiprocessing systems are capable of running multiple processes concurrently. By now such systems have established themselves as the defacto standard for operating systems. At the core of an operating system is the ability to execute programs and as such there must be a primitive for instantiating new processes - also programs are allowed to die/terminate. Operating systems may allow the executing programs to split (spawn) into more computational threads in order to let programs take advantage of concurrent execution as well. One of the most used modelling languages, Timed Automata, is based on multiple automata interacting thus they easily model the concurrent execution of programs. However, this language assumes a fixed size system in the sense that automata cannot be created at will but must be instantiated when the overall system is created. This is in contrast with the fact that developers are able to create threads when needed. In this paper we present our continued work to incorporate spawning of threads into Uppaal

SMC. Our modelling language, Dynamic Networks of Stochastic Hybrid Automata, is essentially Timed Automata extended with a spawning primitive and a tear-down primitive. The dynamic creation of threads has the side-effect that it is no longer possible to use ordinary logics to specify behaviours of individual threads - because the threads no longer have unique names. In this paper we propose an extension of Metric Temporal Logic with means for quantifying over the dynamically created threads. This makes it possible to zoom in on individual threads and specify requirements to their future behaviour. Furthermore, we present a monitoring procedure for the logic based on rewriting formulas. The presented modelling language and the specification language have been implemented in Uppaal SMC version 4.1.18.

Phan Anh Dung : Z3Opt: An optimizing SMT solver

Zhengkui Zhang: Verification and Performance Evaluation of Timed Game Strategies
Joint work with Alexandre David, Huixing Fang, Kim G. Larsen

Control synthesis techniques, based on timed games, derive strategies to ensure a given control objective, e.g., time-bounded reachability. Model checking verifies correctness properties of systems. Statistical model checking can be used to analyse performance aspects of systems, e.g., energy consumption. In this work, we propose to combine these three techniques. In particular, given a strategy synthesized for a timed game and a given control objective, we want to make a deeper examination of the consequences of adopting this strategy. Firstly, we want to apply model checking to the timed game under the synthesized strategy in order to verify additional correctness properties. Secondly, we want to apply statistical model checking to evaluate various performance aspects of the synthesized strategy. For this, the underlying timed game is extended with relevant price and stochastic information. We first explain the principle of translating a strategy produced by Uppaal-tiga into a timed automaton, thus enabling the deeper examination. However, our main contribution is a new extension of Uppaal that automatically synthesizes a strategy of a timed game for a given control objective, then verifies and evaluates this strategy with respect to additional properties. We demonstrate the usefulness of this new branch of Uppaal using two case-studies.