Réseau de recherche franco-québécois sur les mesures quantitatives de la sécurité des systèmes informatiques
Séminaire – 1er et 2 juillet 2014 – LIP6, UPMC

Béatrice Bérard, LIP6, UPMC

3 juillet 2014

Programme

Mardi 1er juillet

9h30-10h00 :	Accueil
10h00-11h00 :	Mathieu Sassolas (avec Quentin Monnet et Lynda Mokdad), *Modeling DoS Attacks in WSNs with quantitative games*
11h00-12h00 :	Olga Kouchnarenko (avec Jean-François Weber) *Decentralised Evaluation of Temporal Patterns over Component-based Systems at Runtime*
12h30-14h00 :	Déjeuner
14h00-17h00 :	Discussion sur le raffinement et la simulation pour les processus de décision markoviens avec intervalles

Mercredi 2 juillet

9h30-10h00 :	Accueil
10h00-11h00 :	John Mullins (avec Béatrice Bérard), *Verification of Information Flow Properties under Rational Observation*
11h00-12h00 :	Béatrice Bérard (avec Olivier Carton), *Channel Synthesis Revisited*
12h30-14h00 :	Déjeuner
14h00-17h00 :	Discussion sur l'opacité pour les processus de décision markoviens avec intervalles

Résumés

• Mathieu Sassolas (avec Quentin Monnet et Lynda Mokdad), *Modeling DoS Attacks in WSNs with quantitative games.*

Wireless sensor networks (WSNs) are made of small devices with low resources, including non-rechargeable batteries. They have been increasingly used for civil applications — urban traffic monitoring or pollution measurement for instance — as well as military ones. In the latter case, they must be resistant to attacks : confidentiality, authentication, and in our case, availability must be ensured.

In this work, we propose to use game theory to model our network. In this setting, the goal of the compromised node is to keep disrupting the network while remaining alive (with sufficiently enough energy). The game studied is a two-player quantitative infinite game on a finite graph, where each transition can change some energy levels and some reward. The goal of the compromised node is hence to maximize its reward while maintaining a positive energy level. The setting of such infinite games aims at modeling what happens in the long run. In addition, games on graphs lack the concurrency of a WSN. As a result, the WSN model has to be adapted to fit into this theoretical model.

On the theoretical side, we show that solving these games is not algorithmically possible if the objective is too complex, namely if it allows both conjunctions and disjunction of requirements on individual dimensions. We can however provide solutions in some restricted cases. The case where the objective is a conjunction of either energy or mean-payoff constraints has been studied in the literature. Here we provide approximate solutions when mixing energy and mean-payoff using *a priori* memory, in keeping with the limited resources of wireless sensors. The ultimate purpose is to demonstrate that, with the presented detection solution, a compromised node cannot win the game, and hence either gets detected, dies, or behaves as a normal (sane) node would.

• Olga Kouchnarenko (avec Jean-François Weber), *Decentralised Evaluation of Temporal Patterns over Component-based Systems at Runtime.*

Self-adaptation allows systems to modify their structure and/or their behaviour depending on the environment and the system itself. Since reconfigurations must not happen at any but in suitable circumstances, guiding and controlling dynamic reconfigurations at runtime is an important issue. This work contributes to two essential topics of the self-adaptation—a runtime temporal properties evaluation, and a decentralization of control loops. It extends the work on the adaptation of component-based systems at runtime via policies with temporal patterns by providing

A specific progressive semantics of temporal patterns and a decentralised method which is suitable to deal with temporal patterns of component-based systems at runtime. The implementation with the GROOVE tool constitutes a practical contribution of this work.

• John Mullins (avec Béatrice Bérard), *Verification of Information Flow Properties under Rational Observation.*

Information flow properties express the capability for an agent to infer information about secret behaviours of a partially observable system. In a language-theoretic setting, where the system behaviour is described by a language, we define the class of rational information flow properties (RIFP), where observers are modeled by finite transducers, acting on languages in a given family $\mathcal{L}$. This leads to a general decidability criterion for the verification problem of RIFPs on $\mathcal{L}$, implying PSPACE-completeness for this problem on regular languages. We show that most trace-based information flow properties studied up to now are RIFPs, hence retrieving several existing decidability results that were obtained by ad-hoc proofs. We introduce rational Orwellian observers and illustrate their power on properties related to selective declassification and conditional anonymity.

• Béatrice Bérard (avec Olivier Carton), *Channel Synthesis Revisited.*

Given a system modeled by a rational relation R, a channel is a pair (E, D) of rational relations that respectively encode and decode binary messages, and such that the composition ERD is the identity relation. This means that the message between E and D has been perfectly transmitted through R.

The problem of channel synthesis asks whether such a pair (E, D) exists and is related to security properties : when the middle process R describes some protocol, the existence of a channel may lead to possibly illegal communication. It is a particular case of distributed synthesis with asynchronous communication, where the synthesis problem is known to be undecidable for general LTL specifications as soon as there are two processes. The channel synthesis problem was also proved undecidable (Σ_1^0-complete) for rational relations, but decidable in polynomial time for a rational function. When a channel exists for such a function, it can be effectively computed.

We revisit this notion of channel and show that it has strong links with rational bijections, hence it is also related to the growth of languages. Given a language L, the growth function associates with an integer $n \geq 0$ the number of words in L of length less than or equal to n. We introduce the notion of *patterns*, which generate typical languages of exponential growth, and establish some of their properties. Then, combining these properties with results on rational bijections, we prove a new characterization for bounded relations with channels : If R is a bounded rational relation, given as a union of rational functions $h_1 + \cdots + h_n$, then the following conditions are equivalent : (1) R has a channel, (2) at least one of the h_is has a channel, (3) the range of R has an exponential growth. We obtain as a corollary that the channel synthesis problem is decidable in linear time for a finite union of functions.