An Overview of FORCES: An INRIA Project on Declarative Formalisms for Emergent Systems

Jesús Aranda[1], Gerard Assayag[4], Carlos Olarte[1,3], Jorge A. Pérez[2], Camilo Rueda[3,4], Mauricio Toro[3], and Frank D. Valencia[1]

[1] INRIA and CNRS-LIX, École Polytechnique.
[2] Dept. of Computer Science, University of Bologna.
[3] Pontificia Universidad Javeriana Cali.
[4] Institut de Recherche et Coordination Acoustique/Musique, IRCAM.

Abstract. The FORCES project aims at providing robust and *declarative formalisms* for analyzing systems in the emerging areas of *Security Protocols, Biological Systems* and *Multimedia Semantic Interaction*. This short paper describes FORCES's motivations, results and future research directions.

Introduction FORCES (FORmalisms from Concurrency for Emergent Systems) is an ongoing project funded by the *Equipes Associées* programme of INRIA. It is carried by the INRIA team COMETE (France), the IRCAM Music Representation Team (France) and the team AVISPA (Colombia). The main goal of FORCES is to provide robust *declarative formalisms* for modeling systems from emergent application areas of computer science in which our teams have been working during recent years: Namely, *Security Protocols, Biological Systems* and *Multimedia Semantic Interaction*.

Process calculi are formalisms that treat communicating processes much like the λ-calculus treats computable functions: The structure of terms reflects the structure of processes and process evolution is represented by term reduction. *Concurrent Constraint Programming* (CCP) based calculi [1] are computational models that combine the operational view of process calculi with a *declarative* one based upon logic.

Some of the members of FORCES developed and used `ntcc` [2], a timed CCP calculus, to predict the behavior of systems from Security Protocols [3], Systems Biology [4] and Multimedia Semantic Interaction [5]. Although these areas differ significantly from one another, there is a crucial commonality in the analysis we wanted to perform in them: *Reachability* i.e., whether a system reaches a particular state. The `ntcc` calculus provides several reasoning tools for reachability analysis. These include a temporal logic, a proof system, verification techniques, and a denotational semantics.

Nevertheless, we have learned from our modeling experience and theoretical studies that `ntcc` is not sufficiently robust for these applications. E.g., some security protocols use a mechanism to allow communication of *nonces* (i.e., uniquely generated random number). The `ntcc` calculus can at best express this mechanism indirectly [6]. Also, `ntcc` lacks constructs for quantitative information, which are essential for biological systems. Furthermore, we have identified musical settings exhibiting complex non-regular timed behavior that cannot be expressed in `ntcc`.

Our research strategy in FORCES has been, with the benefit of hindsight, to develop declarative formalisms for modeling systems from the above-mentioned areas as suitable *extensions* or *specializations* of ntcc. Our expertise in ntcc as well as our modeling experience have been fundamental for guiding our research.

This short paper provides an overview of FORCES. Further information can be found at http://www.lix.polytechnique.fr/comete/Forces.

Declarative Models of Security Protocols A fundamental ability for security protocols is that of generating and communicating private *nonces*; process calculi for security therefore include mechanisms for creating and communicating local names. Neither ntcc nor its predecessor tcc [7] features such mechanisms.

As a remedy to this, in [3] we introduced the Universal Timed CCP process calculus (utcc): a generalization of tcc that allows for the communication of local names (or *links*). This additional expressiveness paves the way for the declarative modeling of a wider class of systems, most notably dynamic ones.

We have endowed utcc with a number of reasoning techniques for reachability analysis. A *symbolic semantics* was defined to deal with problematic operational aspects involving infinitely many substitutions which often arise when modeling security protocols. The semantics uses temporal constraints to finitely represent infinitely-many substitutions; it has been used to exhibit secrecy flaws in some security protocols [3]. The utcc calculus also enjoys a *declarative view* of processes as First-Order Temporal Logic (FLTL) formulae [8]. This allows for reachability analysis of utcc processes using FLTL techniques. For instance, in [3] we used the FLTL formulae representing the model of a protocol to know if it reaches a state where the attacker knows a secret.

We also defined a denotational semantics for utcc [9]. This way, processes can be represented as partial closure operators. As an application of the semantics, we identified a language for security protocols that can be represented as closure operators over a cryptographic constraint system. We showed that the least fixed point of such an operator may then be used to check a secrecy property in a protocol. To our knowledge, this is the first denotational account in the context of calculi for security protocols.

This way, our work has brought new semantic insights into the verification of security protocols, and is related to the research in security protocols from areas closely related to CCP. Namely, Constraint Programming (e.g. [10]) and Logic Programming (e.g. [11,12]). To our knowledge there is no work on Security Protocols that takes advantage of the reasoning techniques of CCP.

Declarative Models of Biological Systems Quantitative information is fundamental for biological systems. For example, behavior in most biochemical reactions is highly dependent on the presence of a certain amount of the substances involved. Very often, information is *partial* as obtaining exact values for parameterizing models is difficult. Unpredictable behavior is thus an inherent condition of the biologic phenomena, and one counts with *partial behavioral information* for describing system interactions. This partial information not only ignores elements on *how* reactions occur (e.g. what components actually interact), but also on *when* such reactions commonly happen (e.g. the relative speeds of the interacting components).

While the notion of partial quantitative information is central to CCP via constraints, partial behavioral information is actually the novelty of ntcc via non-deterministic and asynchronous operators. Our teams have already explored these advantages by analyzing mechanisms for cellular transport and genetic regulatory networks [4,13].

A drawback of these models is their lack of explicit quantitative information. As hinted at above, a fundamental feature of any model of biological systems is the capability of exploiting any available quantitative information. In biological systems this is often represented as *stochastic behavior*. One then has a set of reactions each endowed with a rate representing their propensity or speed. When considering their execution, a race between them takes place and the fastest action is executed.

We have taken initial steps on the inclusion of stochastic information into an explicitly timed concurrent constraint process language [14]. We defined stochastic events in terms of the time units defined by the language: this provides great flexibility for modeling and allows for a clean semantics. Most importantly, by considering stochastic information and adhering to explicit discrete time, it is possible to reason about processes using quantitative logics (both discrete and continuous), while retaining the simplicity of calculi such as ntcc for deriving qualitative reasoning techniques (such as denotational semantics and proof systems). We plan to consolidate the framework outlined in [14], and to apply it to study systems such as the modeled in [15].

Declarative Models of Multimedia Semantic Interaction Interactivity in multimedia systems has become increasingly important. The aim is to devise ways for the machine to be an effective and active partner in a collective behavior constructed dynamically by many actors. In complex forms of multimedia interaction the machine is always adapting its behavior according to the information derived from the activity of the other partners who, in turn, adapt theirs according to the computer actions.

Constructing multimedia systems is thus a challenging task. Their core depends on powerful and consistent concurrent agents architectures. In this setting, ntcc has much to offer. Complex dynamic agent synchronization scenarios can be modeled cleanly and compositionally based on the synchronization mechanism provided by blocking ask constructs. Also, interactions on which little information is available can be conveniently represented using non-determinism. Most importantly, safety properties of the model, crucial in performance settings, can be formally proved to hold.

Quantitative information is also important in musical settings. In [16], we proposed pntcc, the first ntcc extension featuring probabilistic and non-deterministic choices. pntcc advocates the specification of probabilistic, reactive systems within non-deterministic environments. The calculus is equipped with an operational semantics that ensures consistent interactions between both kinds of choices. The semantics is also crucial in the definition of logic-based verification capabilities over system specifications. We have used pntcc for analyzing a scenario of interactive music improvisation (see the extended version of [16]). Probabilitistic information was shown to be useful to obtain a quantitative measure of the quality of an improvised sequence and to enhance the control the modeler has over the whole process.

Interactive scores [17] are models for reactive music systems where weakly defined temporal relations between components specify a hierarchy of loosely coupled music processes. Although the hierarchical structure has been treated as static in previous works, there is no reason it should be so. In [18], we propose a model for dynamic interactive scores where interactive points can be defined to adapt the score depending on the information inferred from the environment (say, a set of performers). We then broaden the interaction mechanisms available for the composer.

In [19] we proposed rtcc, a model of real-time concurrent constraint programming which adds to ntcc the means for specifying and modeling real-time behavior. This calculus has constructs for modeling strong preemption and for defining delays within the same time unit. The operational semantics of rtcc supports resources, limited time and true concurrency. We showed the applicability of the rtcc calculus by giving more faithful models of various musical situations previously modeled in other CCP calculi.

In multimedia interaction settings the real-time execution of models is central. We have implemented a first prototype of an interpreter for ntcc specifications providing real-time interaction with the models developed in the calculus. The tool, called NtccRT [20], also allows for the integration with music composition environments such as OpenMusic (OM, [21]). NtccRT provides a means to write a ntcc specification graphically (using OM) and then to compile it as an standalone program interacting with Midishare [22]. The tool is available at http://ntccrt.sourceforge.net.

Future Directions: Automatic Verification Presently there are no automatic, nor machine-assisted, tools for the simulation and verification of concurrent systems specified in ntcc. Since we deal with complex and large systems, these tools are essential to our intended applications. In fact, the issue of automatic support has received little attention in the case of CCP formalisms. To our knowledge only Villanueva et al (e.g. [23,24]) have addressed automatic verification but in the context of finite-state CCP systems. Several applications of ntcc are, however, inherently infinite-state. Automatic verification of large systems, not to mention infinite systems, is challenging because of the state explosion problem it poses—i.e., the number of states a system has is exponential in the number of processes.

We will take up this challenge by identifying ntcc fragments amenable to automatic verification and by developing techniques and tools to machine assist the verification of system properties in ntcc. We envisage two main complementary approaches for our purposes: (1) Automaton-based and symbolic techniques, and (2) Static and abstract interpretation techniques. We plan to use the automaton representations of processes used to prove the the decidability of the verification problem for ntcc [6], together with the symbolic approach in [3] to ameliorate the state explosion problem. Finally, we expect to develop static and abstract interpretation techniques to extract representative information from system specifications. Such information can be used to reason about essential properties of systems behavior.

We plan to use Security Protocols to test the above-mentioned techniques and tools. In fact, the analysis of Security Protocols is typically carried out using symbolic verification techniques thus making them ideal application candidates. It is also worth noticing that computer simulation plays a fundamental role for Biological Systems because of their inherent complexity. We also plan to develop an ntcc simulation tool and use it as a test bench for (abstractions of) biological systems. We expect that the declarative and parametric nature of ntcc should provide bench biologists with a tool for computing with and analyzing these systems that is intuitive.

References

1. Saraswat, V.A., Rinard, M., Panangaden, P.: The semantic foundations of concurrent constraint programming. In: Proc. of POPL '91, ACM Press (1991)
2. Nielsen, M., Palamidessi, C., Valencia, F.D.: Temporal concurrent constraint programming: Denotation, logic and applications. Nordic Journal of Computing **9**(1) (2002)
3. Olarte, C., Valencia, F.D.: Universal concurrent constraint programing: Symbolic semantics and applications to security. In: Proc. of SAC 2008, ACM (2008)
4. Gutiérrez, J., Pérez, J.A., Rueda, C., Valencia, F.: Timed concurrent constraint programming for analysing biological systems. Electron. Notes Theor. Comput. Sci. **171**(2) (2007)
5. Rueda, C., Valencia, F.D.: A temporal concurrent constraint calculus as an audio processing framework. In: Proc. of SMC 05. (2005)
6. Valencia, F.D.: Decidability of infinite-state Timed CCP processes and first-order LTL. Theor. Comput. Sci. **330**(3) (2005) 577–607
7. Saraswat, V., Jagadeesan, R., Gupta, V.: Foundations of timed concurrent constraint programming. In: Proc. of LICS'94, IEEE CS (1994)
8. Manna, Z., Pnueli, A.: The Temporal Logic of Reactive and Concurrent Systems: Specification. Springer-Verlag (1991)
9. Olarte, C., Valencia, F.D.: The expressivity of universal timed CCP: Undecidability of monadic FLTL and closure operators for security. In: Proc. of PPDP 08. (2008)
10. Bella, G., Bistarelli, S.: Soft constraint programming to analysing security protocols. TPLP **4**(5-6) (2004) 545–572
11. Abadi, M., Blanchet, B.: Analyzing Security Protocols with Secrecy Types and Logic Programs. Journal of the ACM **52**(1) (2005)
12. Millen, J.K.: The interrogator: A tool for cryptographic protocol security. In: Proc. of IEEE Symposium on Security and Privacy. (1984) 134–141
13. Arbeláez, A., Gutiérrez, J., Pérez, J.A.: Timed Concurrent Constraint Programming in Systems Biology. Newsletter of the ALP **19**(4) (2006)
14. Aranda, J., Pérez, J., Rueda, C., Valencia, F.: Stochastic behavior and explicit discrete time in concurrent constraint programming. In: Proc. of ICLP'08. Volume 5366 of LNCS. (2008)
15. Cardelli, L., Gardner, P., Kahramanogullari, O.: A process model of rho gtp-binding proteins in the context of phagocytosis. Electr. Notes Theor. Comput. Sci. **194**(3) (2008) 87–102
16. Pérez, J.A., Rueda, C.: Non-determinism and Probabilities in Timed Concurrent Constraint Programming. In: Proc. of ICLP'08. Volume 5366 of LNCS., Springer (2008) 677–681
17. Allombert, A., Assayag, G., Desainte-Catherine, M.: A system of interactive scores based on Petri nets. In: Proc. of SMC ' 07. (2007)
18. Olarte, C., Rueda, C.: A declarative language for dynamic multimedia interaction systems. In: Proc of. MCM'09, Springer (2009) To appear.
19. Sarria, G., Rueda, C.: Real-time concurrent constraint programming. In: Proc. of CLEI 08. (2008)
20. Toro, M., Rueda, C., Assayag, G., Agón., C.: NtccRT: A Concurrent Constraint Framework for Real-Time Interaction. In: Proc. of International Computer Music Conference. (2009)
21. Bresson, J., Agon, C., Assayag, G.: Openmusic 5: A cross-platform release of the computer-assisted composition environment. In: Proc. of Brazilian Symposium on Computer Music. (2005)
22. D. Fober, Y. Orlarey, S.L. In: Midishare: une architecture logicielle pour la musique. Hermes (2004) 175–194
23. Alpuente, M., Gallardo, M., Pimentel, E., Villanueva, A.: Verifying Real-Time Properties of tccp Programs. Journal of Universal Computer Science **12**(11) (2006) 1551–1573
24. Falaschi, M., Villanueva, A.: Automatic verification of timed concurrent constraint programs. TPLP **6**(3) (2006) 265–300