Modeling and Verification of Evolving Cyber-Physical Spaces

Christos Tsigkanos[1], Timo Kehrer[2], Carlo Ghezzi[3]

Abstract:

In this work, we report about recent research results on the Modeling and Verification of Evolving Cyber-Physical Spaces, published in [TKG17]. We increasingly live in cyber-physical spaces – spaces that are both physical and digital, and where the two aspects are intertwined. Such spaces are highly dynamic and typically undergo continuous change. Software engineering can have a profound impact in this domain, by defining suitable modeling and specification notations as well as supporting design-time formal verification. In this paper, we present a methodology and a technical framework which support modeling of evolving cyber-physical spaces and reasoning about their spatio-temporal properties. We utilize a discrete, graph-based formalism for modeling cyber-physical spaces as well as primitives of change, giving rise to a reactive system consisting of rewriting rules with both local and global application conditions. Formal reasoning facilities are implemented adopting logic-based specification of properties and according model checking procedures, in both spatial and temporal fragments. We evaluate our approach using a case study of a disaster scenario in a smart city.

Keywords: Cyber-Physical Spaces, Dependable Software-Intensive Systems, Safety and Reliability, Modelling and Specification, Formal Verification

Summary

Computing and communication capabilities are increasingly embedded into physical spaces thus blurring the boundary between computational and physical worlds; typically, this is the case in modern cyber-physical systems, like smart buildings or smart cities, hereafter called space-dependent systems. Conceptually, we consider such a composite environment as a cyber-physical space (CPSp), which consists of interrelated computational and physical entities. Like any other software-intensive system, a CPSp is not a static construct. Dynamic actions (e.g. performed by agents) generate continuous change, leading to the notion of an *evolving cyber-physical space*. Thus an evolving CPSp must face the manifold challenges of dynamism – change may affect requirements of the overall space-dependent system.

Formally modeling space and its change as well as reasoning about various properties of evolving space are crucial prerequisites for engineering dependable evolving CPSp. Our approach targets the critical system requirements phase, where a way to obtain formal assurances is highly sought. Elementary properties of an evolving spatial environment can be roughly classified into three kinds; (i) *spatial (local)*, referring to entities forming some structural pattern, (ii) *spatial (global)*, where entities are arbitrarily distributed in

[1] Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano. christos.tsigkanos@polimi.it
[2] Institut für Informatik, Humboldt-Universität zu Berlin. timo.kehrer@informatik.hu-berlin.de
[3] Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano. carlo.ghezzi@polimi.it

space, as well as (iii) *temporal*, expressing system behavior. A plethora of approaches are actively investigated by the community to support reasoning about properties of *one* of these kinds; graphs and graph pattern matching provide suitable methods to deal with local spatial properties, while model checking based on various forms of spatial and temporal logics provides a rigorous approach for the verification of global spatial and temporal properties. However, there is a lack of consideration of *all* of the above listed kinds of properties at the same time. This is a significant deficiency concerning engineering of dependable space-and-time-dependent systems, since properties of interest are often *complex spatio-temporal* properties. Informally, a complex spatio-temporal property refers to behavioral characteristics (temporal) of spatial relationships (spatial; global) of complex structures (spatial; local).

Software engineering (SE) can have a profound impact in engineering of space-and-time-dependent systems, by defining suitable modeling and specification notations as well as supporting design-time formal verification. The typical SE approach –provide a suitable model amenable for analysis and use it to validate a design– is applied to the domain of CPSp. The main contribution of this paper is a technical framework for integrating several fundamental techniques to support reasoning about complex spatio-temporal properties of a model of evolving space. Our modeling approach grounds on Bigraphs [Mi09], a fundamental theory for structures in ubiquitous computing. Local reconfigurations are expressed as rewriting rules called reaction rules, yielding a Bigraphical Reactive System (BRS). Reasoning facilities are implemented adopting logic-based specification of properties and according model checking procedures. Locally bounded spatial properties are expressed as bigraphical patterns, and bigraphical matching is used as a fundamental technique to locate points in space where such formulae hold. For checking of non-local spatial properties, we interpret a bigraphical model as a closure space [Ga03], paving the way for adopting an according spatial logic [Ci14]. Concerning checking of temporal properties, state transition models are obtained from a BRS. We restrict the combination of the above components such that reasoning complexity is manageable and expressiveness is not compromised. We demonstrate applicability using a disaster scenario in a smart city environment.

References

[Ci14] Ciancia, V.; Latella, D.; Loreti, M.; Massink, M.: Specifying and verifying properties of space. In: Theoretical Computer Science. Springer, pp. 222–235, 2014.

[Ga03] Galton, A.: A generalized topological view of motion in discrete space. Theoretical Computer Science 305/1, pp. 111–134, 2003.

[Mi09] Milner, R.: The Space and Motion of Communicating Agents. Cambridge University Press, 2009.

[TKG17] Tsigkanos, C.; Kehrer, T.; Ghezzi, C.: Modeling and verification of evolving cyber-physical spaces. In: Proc. of the 11th Joint Meeting on Foundations of Software Engineering, ESEC/FSE 2017. ACM, pp. 38–48, 2017.