A formal approach to model-driven engineering

Dubravka Ilic and Elena Troubitsyna

Turku Centre for Computer Science (TUCS),
Department of Computer Science, Åbo Akademi University,
FIN-20520 Turku, Finland.

{Dubravka.Ilic, Elena Troubitsyna}@abo.fi

Abstract

Model **D**riven **A**rchitecture (MDA) [5] - a recent initiative of OMG [6] - is gaining increasing popularity in industry. The main idea behind MDA is to develop software-intensive systems by transforming their models expressed in Unified Modeling Language (UML) [8]. Though such an approach facilitates developing systems in a structured way and potentially improves their design, it is yet insufficient for ensuring correctness of the constructed system. In contrast, formal methods have proved to be invaluable for ensuring system correctness but still are rather reluctantly accepted by industry practitioners. In this paper we propose an approach to formalizing MDA-style model transformations in the B Method.

The B Method [1] (further referred to as B) is an approach for the industrial development of correct software. The method has been successfully used in the development of several complex real-life applications [4]. It enables specification, verification and development of a system in a rigorous way. The tool support available for B provides us with the assistance for the entire development process. For instance, Atelier B [3], one of the tools supporting the B Method, has facilities for automatic verification and code generation as well as documentation, project management and prototyping. The high degree of automation in verifying correctness improves scalability of B, speeds up development and, also, requires less mathematical training from the users.

The development methodology adopted by B is based on stepwise refinement [2]. While developing a system by refinement, we start from an abstract formal specification and transform it into an implementable program by a number of correctness preserving steps, called refinements. The top-down design approach advocated by stepwise refinement coincides with the idea of MDA development by model transformations. By integrating these two development paradigms we enhance dependability of the developed systems without losing the visual appeal of diagrammatic UML notations.

In this paper we propose an approach aiming at developing specification and development patterns generic to ad-hoc mobile networks. At first we create templates for modeling ad-hoc networks by expressing the models in UML. Then we translate and verify them in B. We propose a generic development process based on transformations of corresponding models. We verify the correctness of our development by establishing refinement between the corresponding B models.

Our approach allows us not only to reason about correctness of system under construction but also helps in understanding and structuring complex system requirements. Besides, visual nature of the diagrams allows us to easily navigate through the design space and simplifies the process of incorporating changing or emerging requirements into the system. To validate the proposed approach we conducted a case study - model-driven development of routing protocol for ad hoc networks, **A**d hoc **O**n-Demand **D**istance **V**ector (AODV) [7] protocol.

References

[1] J.-R. Abrial. *The B Book: Assigning Programs to Meanings.* Cambridge University Press, 1996.

[2] R.J.Back and J. von Wright. *Refinement Calculus: A Systematic Introduction.* Springer-Verlag, 1998.

[3] ClearSy, Aix-en-Provence, France. *Atelier B - User Manual*, Version 3.6, 2003.

[4] *MATISSE Handbook for Correct Systems Construction*. EU-project MATISSE: Methodologie and Technologies for Industrial Strength Systems Engineering, IST-199-11345, 2003.

Available at http://www.esil.univ-mrs.fr/~spc/matisse/Handbook.

[5] The OMG Model Driven Architecture Official Website: http://www.omg.org/mda/.

[6] The Official Object Management Group Website: http://www.omg.org.

[7] C. E. Perkins, E. M. Belding-Royer, and I. Chakeres. Ad Hoc on Demand Distance Vector (AODV) Routing. *IETF Internet draft*, 2003.

Available at http://moment.cs.ucsb.edu/pub/draft-perkins-manet-aodvbis-00.txt.

[8] J. Rumbaugh, I. Jacobson and G. Booch. *Unified Modeling Language Reference Manual*. Addison Wesley, 1999.