Enhancing Formal Proofs of Network Protocols for Transport Systems using Discrete Event Simulation

Emna Chebbi
Université
du Littoral Cote d'Opale
Email: chebbi@univ-littoral.fr

Patrick Sondi
Université
du Littoral Cote d'Opale
Email: sondi@univ-littoral.fr

Eric Ramat
Université
du Littoral Cote d'Opale
Email: ramat@univ-littoral.fr

***Abstract*—This work proposes a methodology to increase the amount of proven properties of an intelligent transportation system component. A formal tool based on Event-B is used to build a first model of the component and to generate automatically the theorems. Then the model, the theorems and the residual proof obligations (RPO) are incorporated in a discrete event simulation in order to solve interactively some RPO based on simulation results. This paper describes the idea and the challenging issues.**

***Keywords*–Formal Modeling, Simulation, Routing Protocol, Security, Intelligent Transportation Systems.**

I. Introduction

WIRELESS communications technologies are one of the key factors in the development of Intelligent Transportation Systems (ITS). Early deployed in the European Rail Traffic Management System (ERTMS), the Global System for Mobile communications Railway (GSM-R) allows a continuous location and movement management of the trains. However, before GSM-R was adopted in ERTMS, it had to fulfill several specific requirements regarding notably the control-command processes, materialized through the European Train Control System (ETCS) applications, and the security mechanisms, achieved through the Euroradio protocol. While formal methods have been widely used in order to prove the correctness of ETCS applications, the evaluations regarding the GSM-R have been performed essentially by simulation [1] and real-world testing based on key performance indicators. The same trend is now observed in the evaluation of wireless technologies for vehicular networks (VANET), where the evaluations regarding the wireless technology are mostly conducted through simulation and testings, considering mainly performance issues instead of proven properties. The convergence of the main network architectures to the all-IP (Internet Protocol) is pushing both railway operators and car manufacturers to evolve from dedicated infrastructures to a global network connecting all the communicating objects in the smart city. The Internet protocols, initially designed for best-effort applications, are now confronted to the requirements of application domains that are traditionally more sensitive such as tactical units, e-health, and intelligent transport systems. Given the variety of the requirements that could be imposed by such applications, rapid and efficient tools for validating and evaluating custom domain-specific protocols are suitable at the earliest stages of their design. Based on the formal models of the custom protocols designed on top of IP for managing the communications, the research work announced in this paper aims at developing a methodology for obtaining through simulation, not only performance indicators, but also additional formal proofs of some properties attached to both the designed protocols and the entire transport system itself, despite the impairments of the wireless technology.

II. Related work

The design of communication protocols usually relies on a functional model constructed according to the needs of the system. In ITS, the functionalities mainly studied include self-organizing and routing [2], safety and reliability, quality of service, and security. Regarding vehicular networks, several studies have focused on security issues [3]. The increasing number of cyber-attacks over vehicular networks, mainly exploiting protocols weaknesses, have emphasized the need of having robust communications protocols with guaranteed and proven properties regarding security. Several formal models and methodologies have been developed to address that issue, notably in [4] for the verification of security properties of VANET routing protocols. Despite these efforts, there are still some challenging issues, notably the two following, to mention few. The first one concerns the joint evaluation of the components modeled formally with the other components of the ITS. Formal tools such as Event-B allow evaluating only formal model, while simulation tools offer the possibility of connecting heterogeneous models and devices in a single evaluation process. The second one concerns completeness and scalability: formal tools allow animating a limited number of objects in order to verify the behavior of a system in presence of interactions. However, it is difficult to verify large-scale and timed systems. To address this problem, Yacoub and al [5] proposed an approach in order to integrate discrete-event simulation in formal methods. They improved existing model-checking tools by combining them with DEVS simulation in order to allow them detecting the errors that were not previously spotted, especially on timed systems. Though it is a significant step in the resolution of the second issue mentioned previously, it does not address the first.

III. RESEARCH IDEA AND PRELIMINARY WORK

Multi-modeling is a paradigm that allows connecting heterogeneous models, individually based on a different formalism, in a single simulation. DEVS-based multi-modeling has been applied successfully in several simulation based analysis of complex system. Instead of introducing DEVS simulation mechanisms in a formal tool as done in [5], the research idea

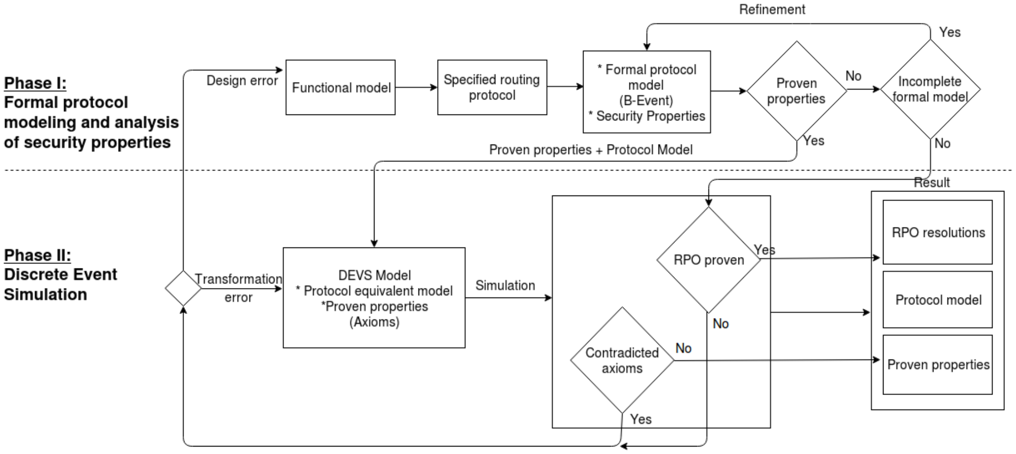

Figure 1. Main steps of a methodology for enhancing the proofs on the properties of an ITS component using Event-B and DEVS

proposed in this work aim at introducing formal models in a multi-modeling development process. In this way, both the components that are modeled with formal methods and the others will be connected in a single simulation of the entire ITS by the mean of multi-modeling. Though this approach would solve the two main issues mentioned in the previous section, it implies three main problems that we propose to solve in our research work:

- problem 1: how the components modeled with a formal tool will be integrated in a ITS multi-modeling?
- problem 2: formal tools include an automatic prover, how multi-modeling approach can manage this?
- problem 3: how multi-modeling simulation could enhance the proofs of the ITS components properties?

Figure 1 describes two major phases of the proposed approach when applied using a formal modeling tool, namely Event-B, and a multi-modeling simulation environment based on DEVS. An ad hoc routing protocol [2], CBL (Chain-Branch-Leaf) designed for vehicular networks is used for illustrating the methodology. The overall operation is to formally model CBL with an Event-B tool in order to prove some of its properties related to security. The automatic prover of the Event-B tool is used in order to build this first set of proven properties, which would solve the problem 2. The next step is to build a DEVS model of CBL that can be guaranteed as rigorously equivalent to the its formal model in the Event-B too. For example, it can be stated that no other assumptions than those used as axioms and those proven as theorem in the formal model can be added in the simulation model. The contributions at this step could solve the problem 1. One key–point is to specify how the proven properties could be taken into account in the simulation model (assumptions, choices, constraints, or parameters ?). With formal modeling through a formalism like Event-B, processes can be executed on the models in order to obtain a list of proven properties that will be guaranteed all the time, and another list containing residual proof obligations (RPO). A former work analyzing a routing protocol with Event-B [6] suggested to discharge the proof obligations interactively. The idea is to find a way to represent each residual proof obligation as a list of queries in DEVS simulation and that could be satisfied using simulation results. Instead of a human agent, the simulation plays the role of the expert. Provided that no other automatic proof is needed between all the different queries related to a residual proof obligation and that all of them are satisfied by the simulation results, the RPO could become a theorem. This could be an answer to the question posed in problem 3. Currently, we are developing a formal model of CBL with Event-B. Specific mechanisms related to security are being introduced in order to verify formally the properties related to mutual authentication between the cluster heads (branch nodes) and their cluster members (leaf nodes). An equivalent model is being developed in a DEVS multi-modeling framework in order to evaluate the efficiency of the first theoretic developments concerning the transfer of Event-B model and theorems of a component to a DEVS simulation multi-modeling of an entire ITS.

IV. Conclusion

This paper presented the first steps of a research idea where formal models are added to a multi-modeling simulation which results are used to solve interactively the residual proof obligations that the formal tool could not automatically demonstrate. The goal is to automatize that interactive resolution.

Acknowledgment

The authors acknowledge the Hauts de France Region.

References

[1] P. Sondi, M. Berbineau, M. Kassab, and G. Mariano, Generating Test Scenarios Based on Real-World Traces for ERTMS Telecommunication Subsystem Evaluation. Springer Berlin Heidelberg, 2013, pp. 223–231.

[2] L. Rivoirard, W. Martine, P. Sondi, M. Berbineau, and G. Dominique, “Cbl : a clustering scheme for vanets,” in The 6th Int. Conference on Advances in Vehicular Systems, Technologies and Applications, 2017.

[3] F. Sakiz and S. Sen, “A survey of attacks and detection mechanisms on intelligent transportation systems: Vanets and iov,” Ad Hoc Networks, vol. 61, 2017, pp. 33–50.

[4] L. Gyesik, “How to formally model features of network security protocols,” International Journal of Security and Its Applications, vol. 8, no. 1, 2014, pp. 423–432.

[5] A. Yacoub, C. Frydman et al., “Using dev-promela for modelling and verification of software,” in Proceedings of the 2016 annual ACM Conference on SIGSIM Principles of Advanced Discrete Simulation. ACM, 2016, pp. 245–253.

[6] D. Méry and N. K. Singh, “Analysis of dsr protocol in event-b,” in Symposium on Self-Stabilizing Systems. Springer, 2011, pp. 401–415.