Software Engineering Group
Department of Computer Science
Nanjing University
http://seg.nju.edu.cn

Technical Report No. NJU-SEG-2012-IC-001

Demo Abstract: BACHOL - Modeling and Verification of Cyber-Physical Systems Online

Lei Bu, Dingbao Xie, Xin Chen,

Linzhang Wang, Xuandong Li

Postprint Version. Originally Published in: ACM/IEEE International Conference on Cyber-Physical Systems 2012, pp.222, IEEE Computer Sciety

Demo Abstract: BACH$_{OL}$ - Modeling and Verification of Cyber-Physical Systems Online

Lei Bu, Dingbao Xie, Xin Chen, Linzhang Wang, and Xuandong Li
State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu, P.R.China 210046
Email: bulei@nju.edu.cn, xdb@seg.nju.edu.cn, {chenxin|lzwang|lxd}@nju.edu.cn

By combining communication, computation and control (3C), Cyber-Physical System (CPS) can generate accurate instructions, achieve complex targets and gain advantages like safety, reliability and efficiency. As mainly of the CPS systems are safety-critical, it is an urgent need to give an efficient technique and tool to guarantee the correctness of the CPS system. Generally speaking, if an accurate model of the system's behavior space can be built, techniques like model checking can be deployed to verify whether any system behavior will violate the given specification.

Nevertheless, as most of the CPS systems are working in open environment, many control parameters used in CPS systems are generated/collected online. The exact values of these variables in any time spot are unpredictable offline in advance. Therefore, the practical engineering model of a CPS system will be a parametric model, which has free parameters included. This causes the behavior of the model has high nondeterminism and is not able to be verified by model checking in the design phase.

To overcome this problem, we proposed that the verification of nondeterministic CPS system should focus on the verification of the system's time-bounded behavior in short-run future (*time-bounded short-run behavior) online* [1]. We propose that the general parametric models which describe the practical behavior of the system should be provided by the designers at first. During system is in operation, a monitor will take charge of collecting the runtime values of these free parameters, then the concrete model can be built by concretizing the parametric model according to the runtime numeric values. After that, the monitor will verify the time-bounded short-run behavior of the model online quickly to predict whether there will be any error in the system's future behavior to guarantee the reliability of the system as shown in Fig.1.

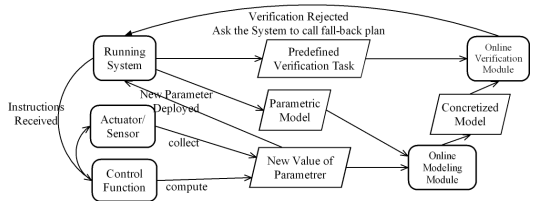

Fig. 1. Online Modeling and Verification Framework

To support the above approach, a toolset BACH$_{OL}$, which is available from http://seg.nju.edu.cn/BACH/, is built based on BACH, which is a bounded model checker for linear hybrid automata (LHA). BACH$_{OL}$ supports the graphical modeling of parametric LHA and provides different APIs to call by monitors online to concertizing parametric models, and performing different kinds of reachability verification on the concrete model as required. In the demonstration, we use a simulation of a real case complex CPS system to show how BACH$_{OL}$ can be deployed online to guarantee the correctness of system behavior by modeling and verifying the system's time-bounded short-run behavior online.

The system used in the demonstration is a communication based train control system (CBTC), which is the state-of-the-art train control system and a typical CPS system. The CBTC system communicates with control center frequently, twice per second, to get the latest movement authority (MA) which indicates the place that the train is permitted to go before receiving a new command. Then the CBTC system will compute the new velocity curve for the next operation cycle autonomously by taking account of the MA it received and the current operation status of the train. During a CBTC system is in operation, there are several safety rules that the system must obey, for example, a train shall never move beyond its MA in each communication cycle. It is obvious that most of the key control parameters mentioned will be computed online and the correctness of these parameters are critical for the safe operation of the running trains.

In the demonstration, we use simulation to show how systems work safely under these rules at first. Then, when some of the control parameters are computed incorrectly, how these rules are broken and trains crash with each other. Next, our tool BACH$_{OL}$ will be deployed into the running system. We show that after the runtime parameters are captured by BACH$_{OL}$, how online models are built and verification are conducted. We can see that when the system is running under the incorrect parameters, BACH$_{OL}$ can find the bug very efficiently and warn the running trains immediately to start a fall-back plan, like emergent braking.

To the best of our knowledge, BACH$_{OL}$ is the first tool that can handle the online modeling and verification of parametric LHA. We believe that by using BACH$_{OL}$, it is applicable to perform the online verification on complex system such as nondeterministic CPS systems to predict error before it happen, and strengthen the reliability of the system.

The authors are supported by the National 863 High-Tech Programme of China(No.2011AA010103), the National Natural Science Foundation of China (No.61100036, No.61003025, No.61170066) and by the Jiangsu Province Research Foundation (BK2011558).

References

[1] L. Bu *et al.*, Toward online hybrid systems model checking of cyber-physical systems time-bounded short-run behavior. In Proceedings of ICCPS11 Work-in- Progress Session.

978-0-7695-4695-7/12 $26.00 © 2012 IEEE
DOI 10.1109/ICCPS.2012.43