Proceedings of the 2013 Winter Simulation Conference
R. Pasupathy, S.-H. Kim, A. Tolk, R. Hill, and M. E. Kuhl, eds

ELAPSED-TIME-SENSITIVE DEVS FOR MODEL CHECKING

Hae Young Lee

Department of Information Security
Seoul Women's University
Seoul, 139-774, Republic of Korea

ABSTRACT

The necessity of formal verification for discrete event system specification (DEVS) has recently arisen mainly due to the application of DEVS to engineering of embedded systems. This paper presents a subclass of DEVS, called *elapsed-time-sensitive* DEVS (ES-DEVS). In order to provide a more convenient and intuitive way to build simulation models for timed systems, conditions on elapsed times are imposed on state transitions caused by input events. While still verifiable, ES-DEVS is more expressive than finite and deterministic DEVS (FD-DEVS) that is another verifiable and deterministic class of DEVS. ES-DEVS models could be exhaustively verified based on reachability analysis techniques.

1 INTRODUCTION

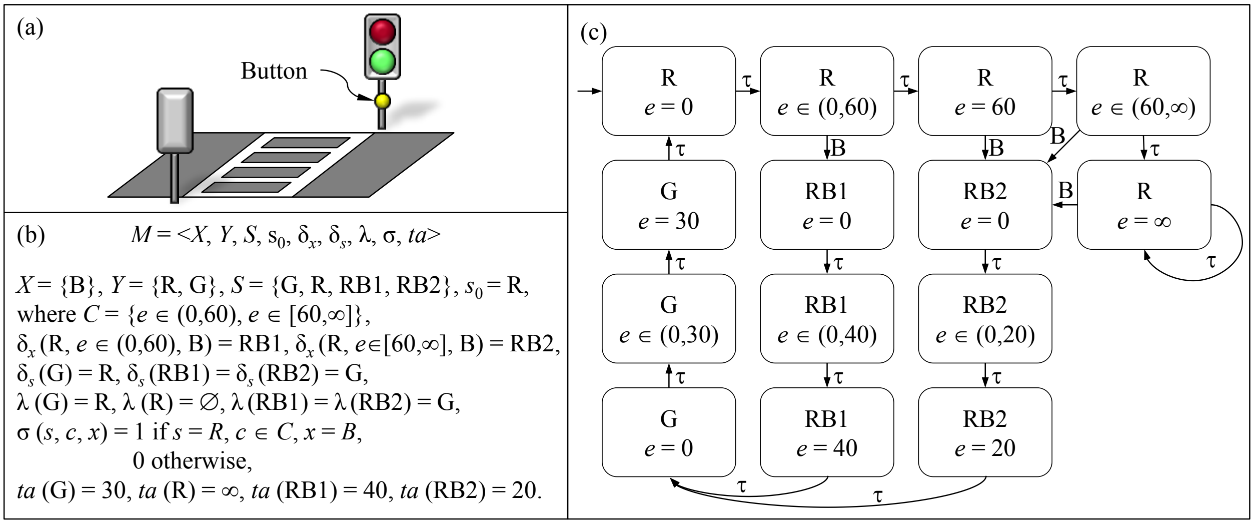
Recently, Hwang and Zeigler (2009) proposed FD-DEVS whose state transitions caused by external stimuli are independent from elapsed times, and a technique to rigidly verify FD-DEVS models through building reachability graphs. It is expected that their research efforts would lay theoretical foundations for formal verification of DEVS (Zeigler, Praehofer, and Kim 2000). However, FD-DEVS requires modelers to make additional efforts in modeling of systems whose external transitions are affected by elapsed times, while most embedded systems (e.g., a controller for a pedestrian crossing shown in Fig. 1(a)) are such ones. This paper presents ES-DEVS, another verifiable subclass of DEVS, in which external transitions can be affected by elapsed times. By imposing constraints on elapsed times, which are used as firing conditions of external transitions, ES-DEVS provides a more convenient and intuitive way to formally describe timed systems, such as embedded systems. Moreover, the expressiveness of ES-DEVS is greater than that of FD-DEVS, while ES-DEVS models could be thoroughly verified based on model checking techniques of timed automata (Alur and Dill 1994). The author is studying to concretize formal verification techniques for ES-DEVS and to develop a modeling and verification tool for it.

2 ES-DEVS AND ITS EXPRESSIVENESS

Let $\mathbb{Q}_{[0,\infty]}$ be the set of non-negative rational numbers with infinity. An *elapsed-time-constraint* (ETC) is formed as $c ::= e \in I$, where $e \in \mathbb{Q}_{[0,\infty]}$ is the elapsed time and I is an interval over $\mathbb{Q}_{[0,\infty]}$. Let C denote the finite set of all ETCs. An atomic ES-DEVS is a structure

$$M = <X, Y, S, s_0, \delta_x, \delta_s, \lambda, \sigma, ta>$$

where X is the finite set of input events, Y is the finite set of output events, S is the finite set of states, $s_0 \in S$ is the initial state, δ_x: $S \times C \times X \rightarrow S$ is the external transition function, δ_s: $S \rightarrow S$ is the internal transition function, λ: $S \rightarrow Y \cup \{\varnothing\}$ is the output function, σ: $S \times C \times X \rightarrow \{0, 1\}$ is the schedule update function, which determines whether event scheduling needs to be performed by ta for external transitions, and ta: $S \rightarrow \mathbb{Q}_{[0,\infty]}$ is the time advance function. Fig. 1(b) shows an atomic ES-DEVS model for a pedestrian crossing controller whose transitions triggered by pressing the buttons are affected by elapsed times. Every atomic FD-DEVS model can be easily transformed into an atomic ES-DEVS one; in case of $C = \{(e \in [0,\infty])\}$, every external transition is independent from the elapsed time, as in FD-DEVS. But some atomic ES-DEVS models cannot be transformed into FD-DEVS ones; for example, the model in Fig. 1(b) cannot be transformed due to an ETC, $e \in (0,60)$. Therefore, the expressiveness of ES-DEVS is greater than that of FD-DEVS, while it can be still deterministic.



(b) $M = <X, Y, S, s_0, \delta_x, \delta_s, \lambda, \sigma, ta>$

$X = \{B\}$, $Y = \{R, G\}$, $S = \{G, R, RB1, RB2\}$, $s_0 = R$,
where $C = \{e \in (0,60), e \in [60,\infty]\}$,
$\delta_x(R, e \in (0,60), B) = RB1$, $\delta_x(R, e \in [60,\infty], B) = RB2$,
$\delta_s(G) = R$, $\delta_s(RB1) = \delta_s(RB2) = G$,
$\lambda(G) = R$, $\lambda(R) = \emptyset$, $\lambda(RB1) = \lambda(RB2) = G$,
$\sigma(s, c, x) = 1$ if $s = R$, $c \in C$, $x = B$,
0 otherwise,
$ta(G) = 30$, $ta(R) = \infty$, $ta(RB1) = 40$, $ta(RB2) = 20$.

Figure 1: (a) a signaled pedestrian crossing, (b) an ETC-DEVS model for its controller, and (c) a region transition system transformed from (b).

3 MODEL CHECKING OF ES-DEVS

As in FD-DEVS (Lee 2013), an ES-DEVS model could be algorithmically transformed into a region transition system (RTS), so that we could directly use model checking techniques of timed automata to rigidly verify ES-DEVS models. For example, the model in Fig. 1(b) can be transformed into an RTS shown in Fig. 1(c). Invariants, which are linear-time properties, can be checked through exploring RTSs. The author is studying to concretize model checking techniques for ES-DEVS, including atomic models and coupled ones, and to develop a model checker based on the techniques.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (NRF-2013R1A1A1006542).

REFERENCES

Alur, R., and D. L. Dill. 1994. “A Theory of Timed Automata.” *Theoretical Computer Science* 126(2):183-235.

Hwang, M. H., and B. P. Zeigler. 2009. “Reachability Graph of Finite and Deterministic DEVS Networks.” *IEEE Transactions on Automation Science and Engineering* 6(3): 454-467.

Lee, H. Y. 2013. “Towards Model Checking of Simulation Models for Embedded System Development.” In *Proceedings of the 19th IEEE International Conference on Parallel and Distributed Systems*.

Zeigler, B. P., H. Praehofer, and T. G. Kim. 2000. *Theory of Modeling and Simulation*. 2nd ed. Academic Press.