Delayed Hybrid Systems

Erzana Berani Abdelwahab*

Carl von Ossietzky Universität, Oldenburg, Germany.
erzana.berani.abdelwahab@uni-oldenburg.de

Introduction and Related Work. The increasing range of applications in technology where the physical environment is constantly interacting and automatically being monitored by embedded computers, has led to an ample research on hybrid systems as a formal model for design and analysis of such embedded control systems. A hybrid system is a composition of discrete modes representing the control mode and ordinary differential equations (ODE) representing the continuous evolution of physical activities inside each operating mode of the system. As these discrete-continuous interactions between the embedded computers and the physical world may often become complex and safety-critical, there is an urgent need in improving the accuracy of representing this tight relation between the two components in simulatable models, and complementing it with reliable automatic verification techniques.

A significant factor which has direct implications and is often neglected in the model design is the feedback delay, although it naturally arises in feedback loops in modern forms of embedded digital control, like networked control systems. With outdated information due to delays in receiving data from sensors, and similarly not being able to apply control actions on time due to delays in actuator channels, delays cause overshoots and oscillations which often invalidate both the stability and safety certificates obtained from delay-free models. While resulting in more accurate models, delays inherently induce extra complexity which in turn prevents straightforward generalizations of the already established automatic verification methods for delay-free hybrid systems [1]. This delay-induced complexity comes from the fact that the evolution of dynamics is no longer dependent on the current state only, but depends on an infinite sequence of states during a finite time interval in the past, and thus resulting in an infinite-dimensional dynamical system. This shows that one of the main challenges in solving the reachability and verification problem for delayed dynamics is to find a computationally feasible way to represent and store the history information which is going to govern the current evolution of the dynamics. The research community has already made attempts to tackle these challenges in purely continuous systems where they exploited the model of Delay Differential Equations (DDE). Such a DDE with punctual delays takes the shape

$$dx(t)/dt = f(x(t), x(t-\delta_1), ..., x(t-\delta_n)),$$

where the δ_i are positive constants. These attempts have resulted in several verification approaches for dynamical systems represented by DDEs [2-4].

* PhD Supervisor: Martin Fränzle

Recently, delays have also been considered in discrete-time and discrete-state systems where delayed observation and actuation in finite-state automata has led to interesting results on strategy synthesis for discrete safety games [5,10]. However, it is surprising that despite a large portion of digital control schemes being an integration of discrete and continuous state dynamics, i.e., hybrid state dynamics, there are as yet no similar developments for controlling and verifying hybrid systems subject to delays. In [6] sufficient conditions on stabilization of hybrid stochastic systems under input delays are obtained. In this model there is always at most one delayed switch that is latent, i.e., delayed discrete transition, which in timed automata could also be easily modeled by starting a clock in every switch and performing the action after a certain time reached by the clock. In our model however, we model the pipelining of events within communication networks, such that, multiple delayed switches referring to different events queuing in the network, may coexist simultaneously. This is modelled by transitions being guarded by presence of a certain event exactly δ time units ago: in a timed I/O-automaton with delays, a transition $l \rightarrow \mathrm{a}(-\delta)/\mathrm{b} \rightarrow l'$ would permit a move from l to l' together with generation of output event b iff input event a has been present exactly $-\delta$ time units ago. In this way, by referring directly to the events in the past (e.g., whenever an X event happened Y time units ago, a certain action is performed), our model can memorise reactions to arbitrarily many arbitrarily close events and perform the corresponding action to each event. These actions are essentially queued in the order that the corresponding events happened in the past. Thus, the delay form we aim to model is a richer expression of delay through which no event can go undetected as a result of being too close to another event that has just been detected, or happening simultaneously with another event.

Motivated by the above observations, introducing a formal semantic, i.e., mathematical model for rigorously modeling delays arising in hybrid systems thus constitutes the main objective of this PhD project. Using the recent results, DDEs shall be used for modeling the continuous dynamics with a potentially enhanced accuracy through considering a distributed version of delays, where delayed variables do not refer to a single point in the past, but rather to a convolution of the past solution with a windowing function, thus integrating over periods of the past. The general shape is given by the distributed DDE

$$dx(t)/dt = f\left(x(t), \int_0^{-\delta} g\left(x(t-s), s\right) ds\right),$$

where g is a windowing function and δ a positive constant. The windowing function could be a simple mask like $g(x,s) = x$ for all $s \in$ [-δ,0] or a smooth window like the Hamming window. On the other side, the discrete-continuous interface requires a reasonable notion of delayed triggering of discrete transitions, suitable for distributed network systems, to be defined as well. First findings indicate that even for simple automata classes, like timed automata, the reachability problem becomes undecidable once pipelined delays are introduced. Observing that the delay form described above cannot be modeled by a finite number of clocks, undecidability properties come as a natural consequence when composing timed automata with this type of delay. A reasonable model of delayed automata thus is a prerequisite of our theory. Once this model is established, our aim is to develop verification techniques for delayed hybrid systems.

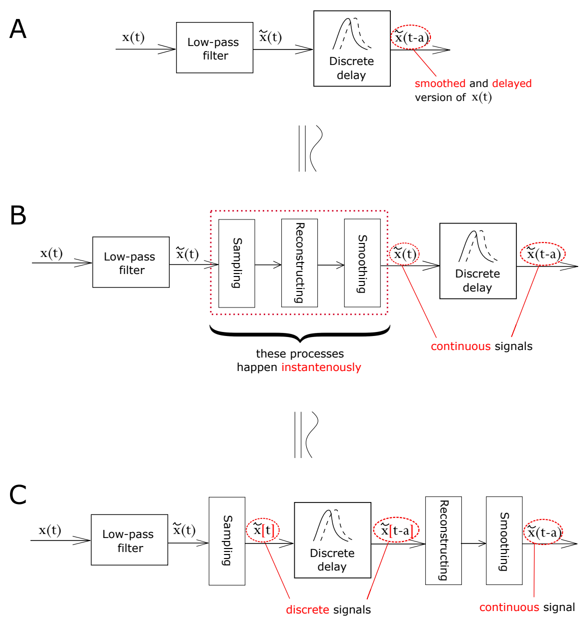

Fig. 1. Distributed delays can be modeled by combining a discrete delay with a low-pass filter **(1.A)**. As long as the continuous input signal $x(t)$ is band-limited, the sampling theorem then enables us to reconstruct the original signal from a finite number of samples in exact and continuous form **(1.B)**. Using the linearity property of the delay block, one obtains the exact same output even when the delay block is replaced between the sampling and reconstructing blocks. However, with this new arrangement of blocks, instead of remembering the infinitely many points from the past, we end up reconstructing the whole infinitesimal history by remembering only a finite number of points **(1.C)**.

Current stage of research. The recent results on DDEs, despite constituting a major step toward successful analysis and verification of continuous dynamics subject to delays, share a common limitation on their assumption that delays are constant and discrete; namely, given a constant fixed delay δ, it is assumed that the state at every instant of time, $x(t)$, is dependent on the previous state exactly δ time units in the past, $x(t-\delta)$. However, most of the engineering practice find punctual delays an overidealization when integrating them in the model design. In [7] Toyota researchers have proposed a verification benchmark where in particular the air-fuel ratio control is governed by a DDE, which comes from the fact that the exhaust gas produced by the engine takes some time to reach the oxygen sensor, i.e., it induces a transport delay. However, since exhaust gas gets compressed and mixed by turbulences down the exhaust pipe, in the Simulink model [9] "smoothed" delays are implemented instead of discrete point delays.

Motivated by the benchmark in [7] and the interesting decidability results obtained once punctuality is relaxed [8], currently we are exploiting the idea of using distributed delays as a more relevant model and potentially easier to analyze compared to discrete delays. The smoothing effect embedded in distributed delays implies promising results in reconstructing the history segment based on finite samples. This is due to the presence of low-pass filter which enables us to use the Sampling Theorem and thus reconstruct the continuous delayed signal from only a *finite* number of samples (See **Fig.1**). Thus, this approach ultimately leads to the reduction of a DDE problem to that of solving an, albeit higer-dimensional, standard ODE. Future work will exploit this reduction for automatic verification of hybrid systems incorporating distributed delays.

References

1. M. Fränzle, M. Chen, and P. Kröger. In Memory of Oded Maler: Automatic reachability analysis of hybrid-state automata. *ACM SIGLOG News*, 6(1):19-39, 2019.
2. Z. Huang, C. Fan, and S.Mitra. Bounded invariant verification for time-delayed nonlinear networked dynamical systems. *Nonlinear Analysis: Hybrid Systems*, 23:211-229, 2017.
3. B. Xue, P.N. Mosaad, M. Fränzle, M. Chen, Y.Liu, and N. Zhan. Safe over- and under-approximation of reachable sets for delay differential equations. In *FORMATS'17*, vol. 10419 of *Lecture Notes in Computer Science*, pp. 281-299, 2017.
4. E. Goubault, S. Putot, L. Sahlmann. Inner and outer approximating flowpipes for delay differential equations. In *CAV'18*, vol. 10982 of *Lecture Notes in Computer Science*, pp. 523-541, 2018.
5. M. Chen, M. Fränzle, Y. Li, P.N. Mosaad, and N. Zhan. What's to Come is Still Unsure. In *International Symposium on Automated Technology for Verification and Analysis*, pp. 56-74. Springer, Cham, 2018.
6. S. Luo, and F. Dend. Stabilization of hybrid stochastic systems in the presence of asynchronous switching and input delay. *Nonlinear Analysis: Hybrid Systems*, 32:254-266, 2019.
7. J. Xiaoqing, J.V. Deshmukh, J. Kapinski, K. Ueda, and K. Butts. Powertrain control verification benchmark. In *Proceedings of the 17th international conference on Hybrid systems: computation and control*, pp. 253-262. ACM, 2014.
8. R. Alur, T. Feder, and T.A. Henzinger. The benefits of relaxing punctuality. *Journal of the ACM (JACM)*, 43(1):116-146, 1996.
9. J.V. Deshmukh. Simulink/Stateflow models of the Powertrain control verification benchmark. Personal Communication.
10. M. Zimmermann. Finite-state strategies in delay games. In: P.Boyer, A.Orlandini, and P.San Pietro editors, *8th Symposium on Games, Automata and Formal Verification (GandALF'17)*, vol. 256 of *EPTCS*, pp. 151-165, 2017.