Water Level Control (CAV 2010)

AVACS H4
Phase 2

July 28, 2011

1 Description of the Model

This case study is related to our CAV paper [4]. We consider a model of a water level control system using wireless sensors. This model is an extension of the one described in [1]. Values submitted are thus subject to probabilistic delays, due to the unreliable transport medium. A sketch of the model is given in Figure 1. The water level y of a

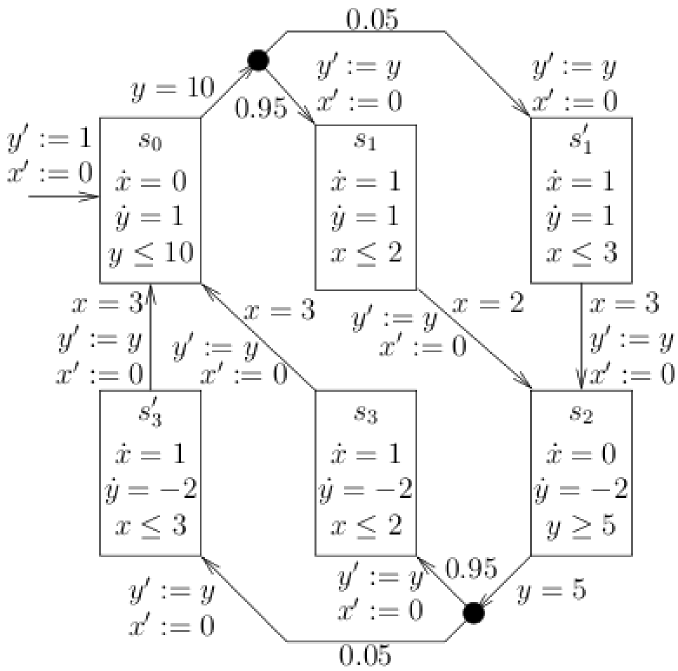

Figure 1: CTMDP of the Water Level Control System

tank is controlled by a monitor. Its change is specified by a linear function. Initially, the water level is $y = 1$. When no pump is turned on (s_0), the tank is filled by a constant stream of water ($\dot{y}$). When a water level of $y = 10$ or above is seen by a sensor of the tank, the pump should be turned on. However, the pump features a certain delay, which results from submitting control data via a wireless network. With a probability of 0.95 this delay takes 2 time unites (s_1), but with a probability of 0.05 it takes 3 time units (s_1'). The delay is realized by the timer x. After the delay has passed, the water is pumped out with a higher speed than it is filled into the tank ($\dot{y} = -2$ in s_2). Another sensor perceives whether the water level is below 5 and turns the pump off again. Again, we have a distribution over delays here (s_3 and s_3'). For the system to work correctly, the water level must stay between a value of 1 and 12.

We are interested in the probability that the pump system violates the property given above, that is either the water level falls below 1 or grows above 12, within a given time bound T.

2 Results

We model the previously described system in *ProHVer* [2] and reason about this property: performance statistics are given in Table 1. Without using partitioning, we were only able to obtain exact values for time bounds up to 82. Notice that we did not use the convex hull over-approximation [3] nor another over-approximation. For time bounds larger than this value, we always obtained a probability limit of 1. To get tighter results, we partitioned x by an interval of length 2. For time bounds below 83 we obtain the exact value in both table parts, whereas for 83 we obtain a useful upper bound only when using partitioning. A plot of probabilities for different time bounds is given in Figure 2. The graph has a staircase form where wide steps alternate with narrow ones. This form results, because each time the longer time bound was randomly chosen, the tank will overflow or underflow respectively, if there is enough time left. The wide steps corresponds to the chance of overflow in the tank, the narrow ones to the chance of underflow.

References

[1] Rajeev Alur, Costas Courcoubetis, Nicolas Halbwachs, Thomas A. Henzinger, Pei-Hsin Ho, Xavier Nicollin, Alfredo Olivero, Joseph Sifakis, and Sergio Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138:3–34, 1995.

[2] Martin Fränzle, Ernst Moritz Hahn, Holger Hermanns, Nicolás Wolovick, and Lijun Zhang. Measurability and Safety Verification for Stochastic Hybrid Systems. In *HSCC*, pages 43–52, New York, NY, USA, 2011. ACM Press.

[3] Goran Frehse. PHAVer: Algorithmic Verification of Hybrid Systems Past HyTech. In Manfred Morari and Lothar Thiele, editors, *Hybrid Systems: Computation and Control*, volume 3414 of *LNCS*, pages 258–273. Springer, 2005.

Time bound	No partitioning Probability	 Build (s)	 Abstract states
40	0.185	0	69
82	0.370	0	283
83	1.000	1	288
120	1.000	1	537
500	1.000	38	3068
1000	1.000	169	6403

Time bound	Interval of length 2 Probability	 Build (s)	 Abstract states
40	0.185	1	150
82	0.370	2	623
83	0.401	2	640
120	0.512	4	1220
500	0.954	79	7158
1000	0.998	365	14977

Table 1: Results of *ProHVer* With/Without Partitioning

[4] Lijun Zhang, Zhikun She, Stefan Ratschan, Holger Hermanns, and Ernst Moritz Hahn. Safety Verification for Probabilistic Hybrid Systems. In *CAV*, volume 6174 of *LNCS*, pages 196–211. Springer, 2010.

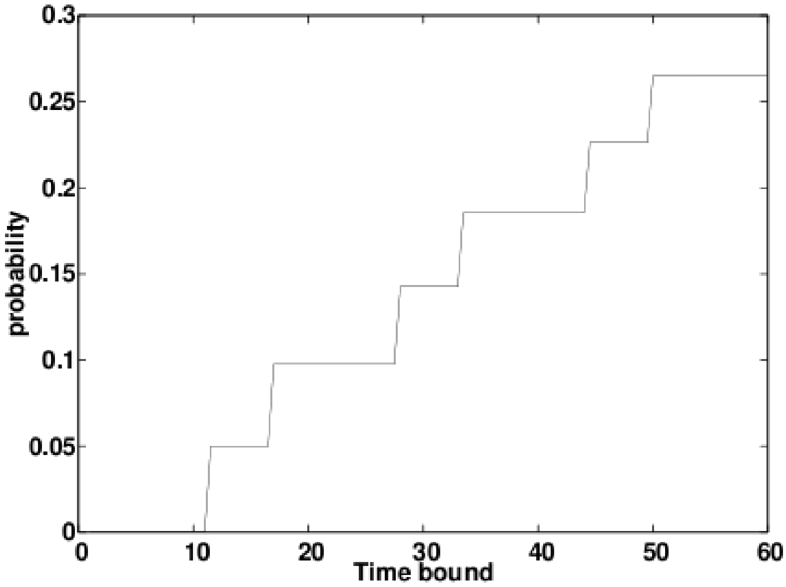

Figure 2: Plot of Error Probabilities