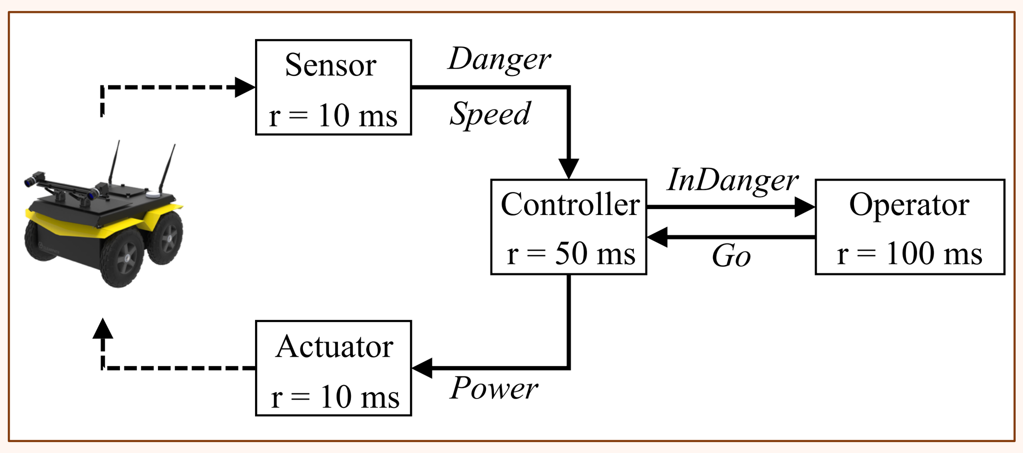
SOFTWARE ANALYSIS RESEARCH LABORATORY

SCHOOL OF COMPUTING
UNIVERSITY OF UTAH

Toward Liveness Verification of Quasi-Periodic Distributed Systems Using a Timeless Model

M. Dabaghchian*, Z. Rakamarić
*maryam@cs.utah.edu

Motivating Example



Safety properties
- No collision
- Speed in a valid range

Verification Using Model Checking

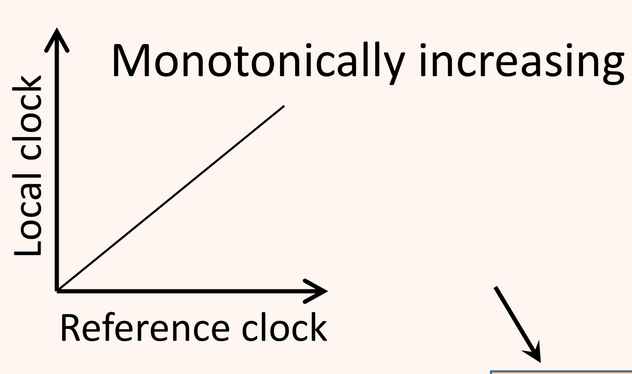
s: program state (variables' valuation) **t**: clock value

s,t —Discrete transition→ s',t s,t —Delay transition→ s,t'

Continuous time model
- Time is a real value and advances continuously
- Infinitely many delay transitions between two discrete events

Discrete time model
- Time is a real value and jumps to the time of the next event
- Finite delay transitions between two discrete events

Problem Statement



s,t —Delay transition→ s,t'

$t \in \mathbb{R}$

Infinite state space
∞

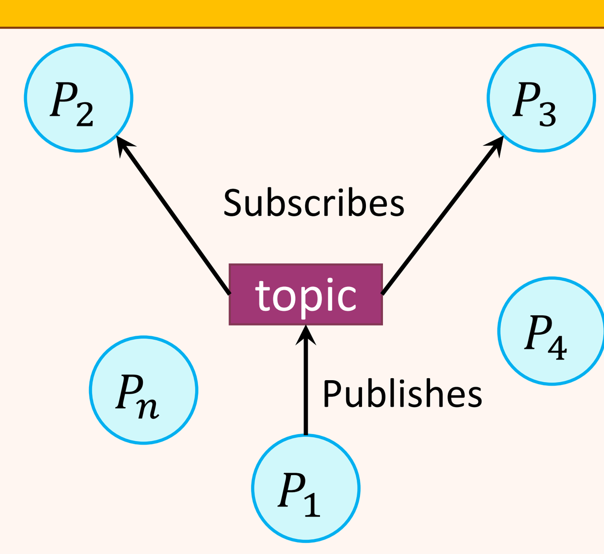
Solution: eliminate time notion
- So that we can use any regular discrete event model checker, such as SPIN

Quasi-Periodic Distributed System (QPDS)

Every process
- Activation period
- Local clock with a bounded drift

Processes
- Communicate through publish-subscribe pattern
- Bounded message transmission delay

A process
- Gets activated
- Reads messages from all its receiving buffers
- Performs a local computation
- Publishes messages



Quasi-synchrony: Discrete time abstraction for single-rate QPDSs [Caspi 2000]

Computational model for multi-rate QPDSs [Larrieu and Shankar 2014] → Soundness of the abstract model – constrain communication topology [Baudart et al. 2016]

Calendar Model

Calendar set: C

$< e_1, \tau_1 > \ldots < e_n, \tau_n >$
$<< p', \epsilon, \epsilon >, ct >$
$<< p, t, m >, ct >$

Set of pairs of events and their timeouts.

e	event
$\tau \in \mathbb{R}_{\geq 0}$	timeout
$ct \in \mathbb{R}_{\geq 0}$	Global current time

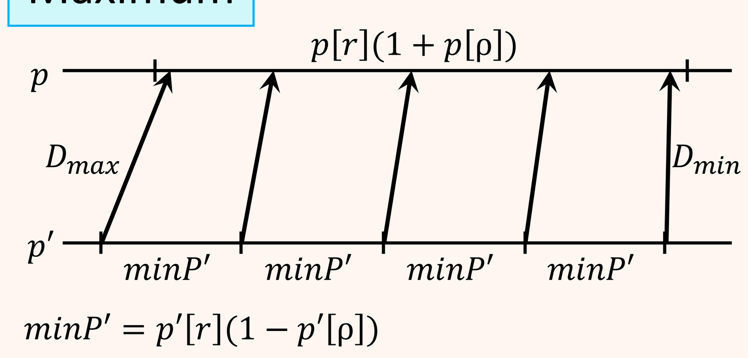
$< p, t, m >$	Message delivery event
$< p, \epsilon, \epsilon >$	Process activation event

Calendar invariant: $\forall < e, \tau > \in C.\ ct \leq \tau$

Constraint Satisfaction Problem

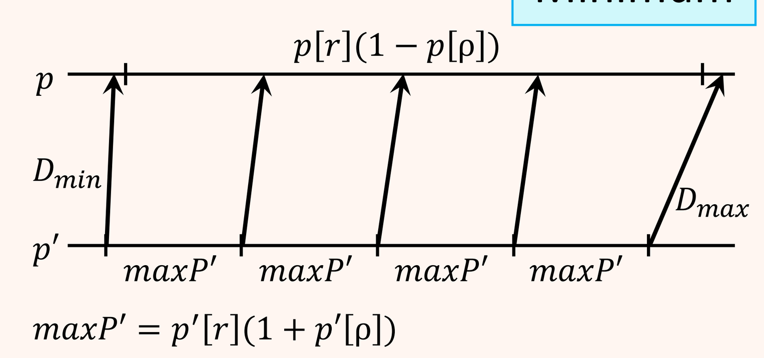
Number of messages received by p

Maximum



Buffer sizes have to be sufficient to limit the maximum number of lost messages

Minimum



Buffer sizes have to be sufficient to hold the minimum number of messages

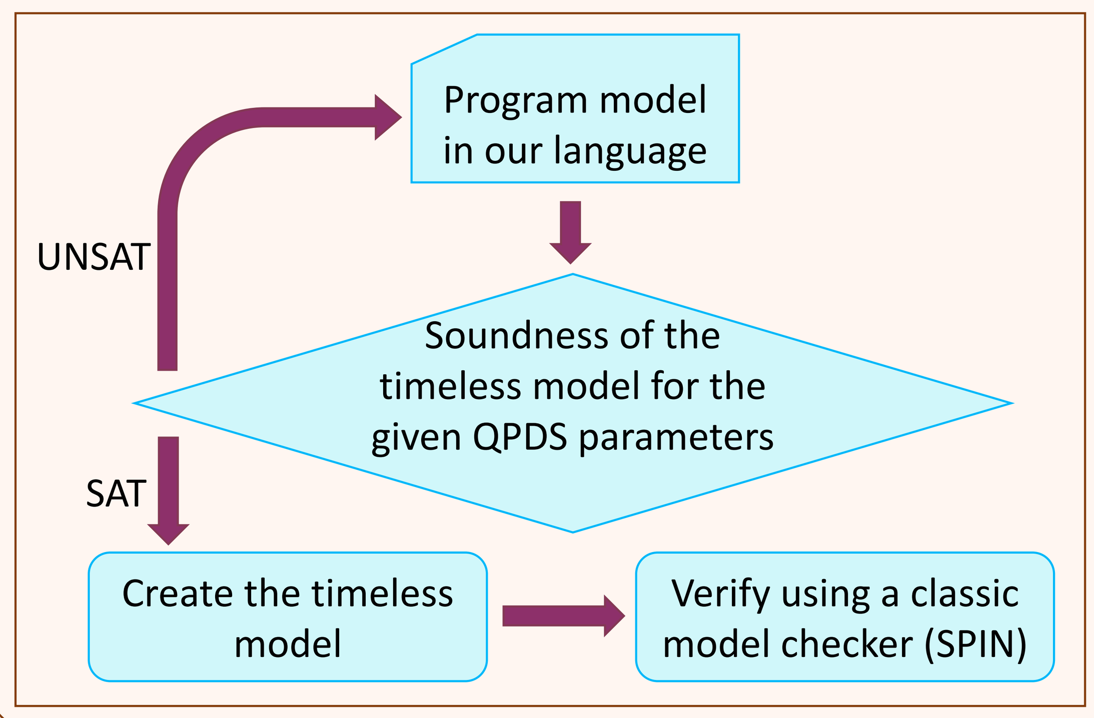
Timeless Model

Communication channels: ζ

$\zeta(p,t)$ Buffer

A process can publish a message m to the topic t ($publish(t,m)$)
if
it will not violate the maximum number of lost messages

Workflow



Overapproximation

Timeless model
Calendar model

Proof is reduced to stuttering equivalence relation between two execution traces

Completeness

Timeless model overapproximates the calendar model
- False alarms for safety properties
- Not suitable for checking of liveness properties

Unfair behavior
- A subscriber process is activated more often than all its publishers, e.g., Actuator and Controller

Count the number of process activations, where required

Eliminate processes with no impact on the environment

Their combination

Adding fairness and capability of liveness properties checking is work in progress.

Conclusion

Synchronization

	Real-time System	Calendar Model	Timeless Model
Synchronization	Local clocks with bounded drifts	Global clock	Buffers' length

References

- Paul Caspi. 2000. The quasi-synchronous approach to distributed control systems. Technical Report. Verimag, Crysis Project
- R. Larrieu and N. Shankar. 2014. A framework for high-assurance quasi- synchronous systems. In Proceedings of the 12th International Conference on Formal Methods and Models for Codesign. 72–83. https://doi.org/10.1109/MEMCOD.2014. 6961845
- Guillaume Baudart, Timothy Bourke, and Marc Pouzet. 2016. Soundness of the Quasi-synchronous Abstraction. In Proceedings of the 16th International Confer-enceonFormalMethodsinComputer-AidedDesign.9–16. https://doi.org/10.1109/ FMCAD.2016.7886655