Metric Temporal Logic with Resettable Skewed Clocks
(Extended abstract)

Alberto Bombardelli, Stefano Tonetta

Embedded Systems Unit, Fondazione Bruno Kessler, Italy

MOTIVATION

Distributed Real Time System (DRTS):
- **Multiple components**
- **Message passing and timing constraints**
- **Local time semantics** (skewed clocks)
- **Properties expressed with LTL and MTL**
- **Clock synchronization** $\Rightarrow$ Non-monotonic time

Compositional verification:

$$\Big(\bigwedge_{c_i \in Comps} \underbrace{\varphi_{c_i}}_{\text{comp behaviour}}\Big) \rightarrow \underbrace{\varphi}_{\text{global property}}$$

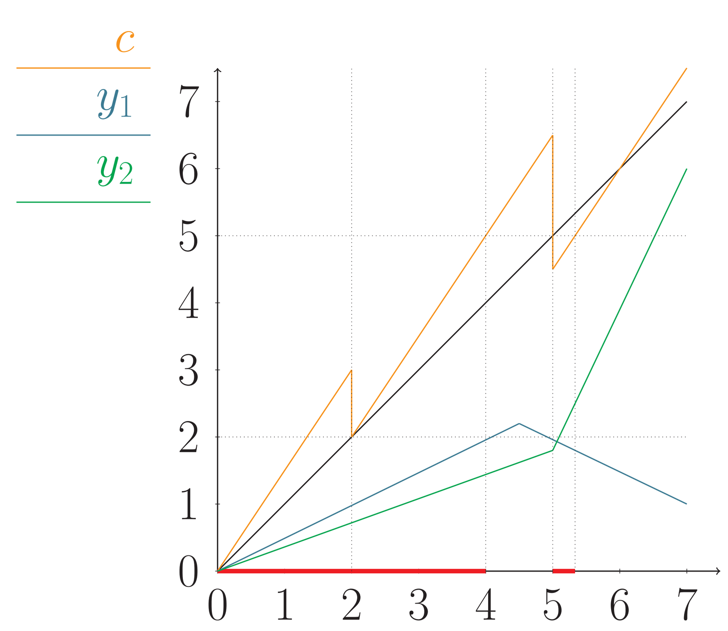
MTL

Syntax : $\phi := p \mid \phi \vee \phi \mid \neg\phi \mid X\phi \mid \phi_1 U_{\mathcal{I}} \phi_2$ where $\mathcal{I}$ is an interval of $\mathbb{R}_0^+$

Semantics:

$\pi, t \models \varphi U_{\mathcal{I}} \psi \Leftrightarrow$ exists $t' > t$, s. t. $\nu(t') - \nu(t) \in \mathcal{I}, \pi, t' \models \psi$, and for all $t \leq t'' < t : \pi, t'' \models \varphi$

NON-MONOTONICITY OF TIME



- Distributed MTL: $U_{\mathcal{I}}^c$
- Time can decrease with resets
- Harder to verify (need to check disjointed intervals)
- Intervals of $\mathbb{R}$ instead of $\mathbb{R}_0^+$

- $\varphi_i := G^c_{\leq 5}(y_i \leq 2)\ \forall i \in \{1,2\}$
- φ_i holds iff $y_i \leq 2$ holds in [0,4] and [5, 16/3]

MTLSK

Syntax:

MTLSK : $\phi := \cdots \mid \phi_1 U^c_{\mathcal{I}} \phi_2 \mid \phi_1 \overline{U}^c_{\mathcal{I}} \phi_2$ where $\mathcal{I}$ is an interval of $\mathbb{R}$

Semantics:

$\pi, t \models \varphi U^c_{\mathcal{I}} \psi \Leftrightarrow$ exists $t' > t$, s. t. $\pi(t')(c) - \pi(t)(c) \in \mathcal{I}, \pi, t' \models \psi$, and for all $t \leq t'' < t : \pi, t'' \models \varphi$

$\pi, t \models \varphi \overline{U}^c_{\mathcal{I}} \psi \Leftrightarrow$ exists $t' > t$, s. t. $\pi(t')(c) - \pi(t)(c) \in \mathcal{I}, \pi, t' \models \psi$, and for all $t \leq t'' < t : \pi, t'' \models \varphi$ and $\pi(t'')(c) - \pi(t)(c) \in \mathcal{I}^-$ where $\mathcal{I}^- := \mathcal{I} \cup (-\infty, inf(\mathcal{I})]$

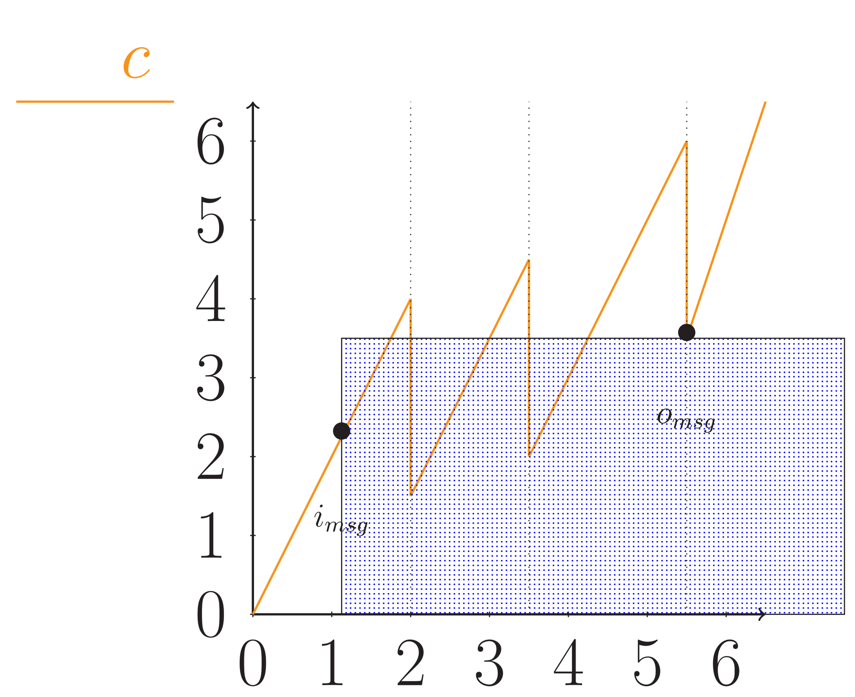
Properties:

$\pi \models \varphi \overline{U}^c_{\mathcal{I}} \psi \Rightarrow \pi \models \varphi U^c_{\mathcal{I}} \psi$, If $sup(\mathcal{I}) = +\infty : \pi \models \varphi \overline{U}^c_{\mathcal{I}} \psi \Leftrightarrow \pi \models \varphi U^c_{\mathcal{I}} \psi$

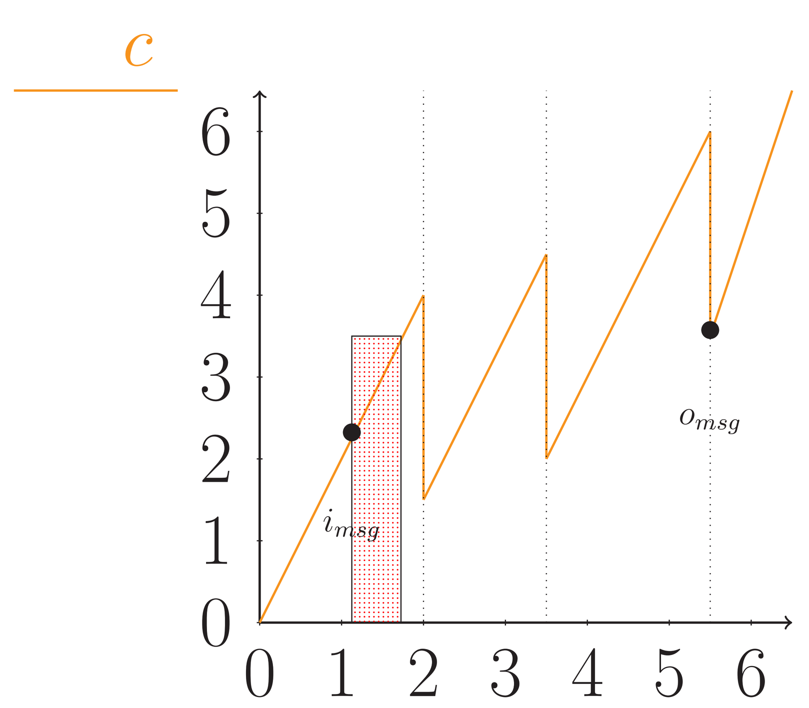
If there is no **reset**: $\pi \models \varphi \overline{U}^c_{\mathcal{I}} \psi \Leftrightarrow \pi \models \varphi U^c_{\mathcal{I}} \psi$

If c is a **perfect** clock: $\pi \models \varphi \overline{U}^c_{\mathcal{I}} \psi \Leftrightarrow \pi \models \varphi U^c_{\mathcal{I}} \psi \Leftrightarrow \pi \models \varphi U_{\mathcal{I}} \psi$

F^c AND $\overline{F}^c$ COMPARISON:

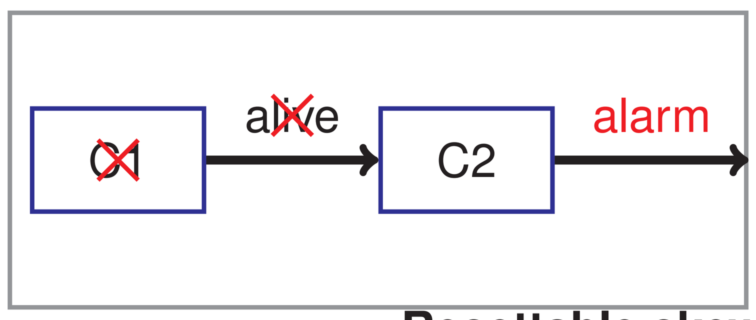


$\varphi_{blue} := G(r(i_{msg}) \rightarrow F^c_{\leq 5/4} s(o_{msg}))$



$\varphi_{red} := G(r(i_{msg}) \rightarrow \overline{F}^c_{\leq 5/4} s(o_{msg}))$

EXAMPLE



Perfect clock example

$G(fault \rightarrow G^{cl1}_{\leq p} \neg alive) \wedge$
$G(G^{cl2}_{\leq p} \neg alive \rightarrow F^{cl2}_{\leq p} alarm) \rightarrow$
$G(fault \rightarrow F^{cl}_{\leq p} alarm)$

Valid if all clocks are perfect

Resettable skewed clock example

$G(fault \rightarrow G^{cl1}_{\leq p} \neg alive) \wedge$
$G(G^{cl2}_{\leq p - 4\tilde{q}} \neg alive \rightarrow F^{cl2}_{\leq p} alarm) \rightarrow$
$G(fault \rightarrow F^{cl}_{\leq p + 2\tilde{q}} alarm)$

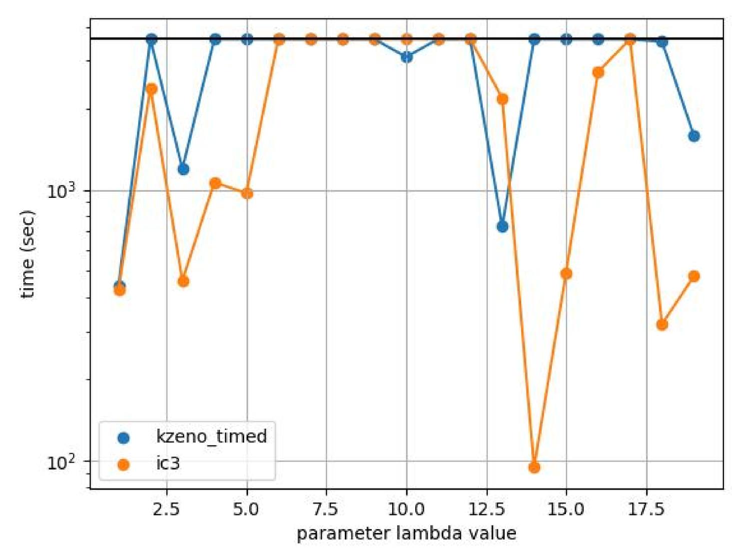
where $\tilde{q} = q(1 + 2\epsilon/(1-\epsilon))$

Valid if $cl1$ and $cl2$ synchronized with cl every q time units

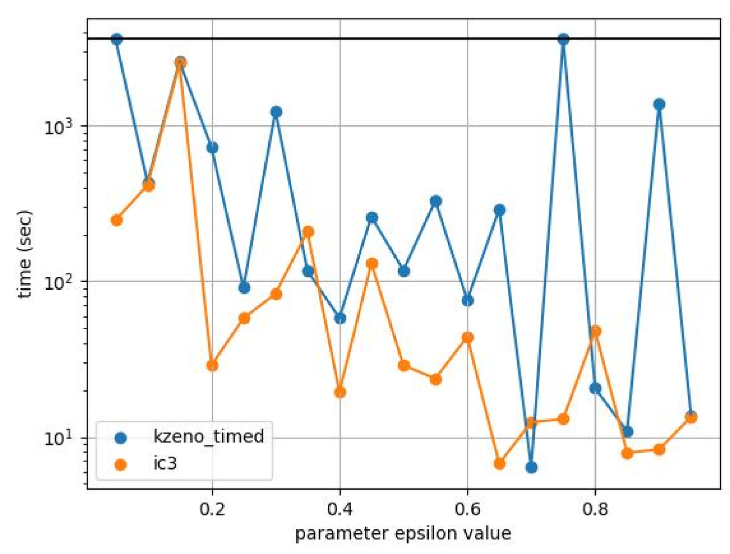
RESULTS (FROM [2])

Implementation:
- Parametric fragment of **MTLSK** (interval semantics)
- Implemented inside timed nuXmv[4]
- Algorithm ic3-ia[5] and kzeno[6] (in lockstep with BMC)

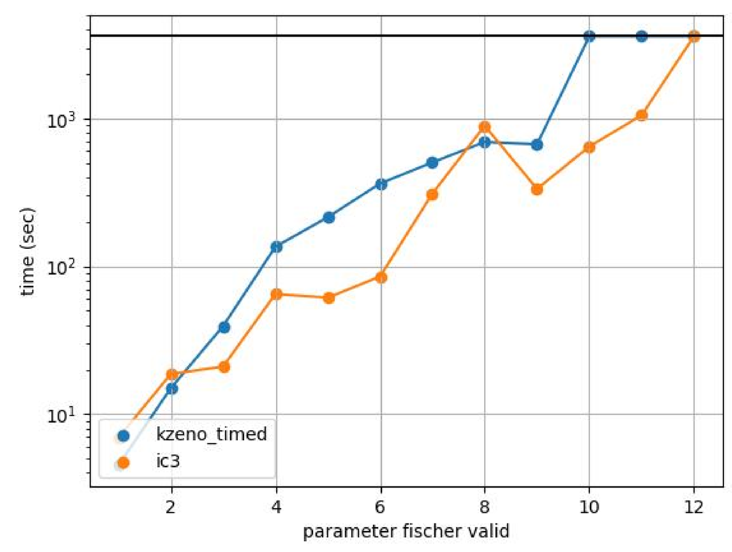
Experiments:
- Instantiation of λ and ϵ
- Parametric bounded response pattern
- Fischer algorithm (from [4] experimental evaluation).



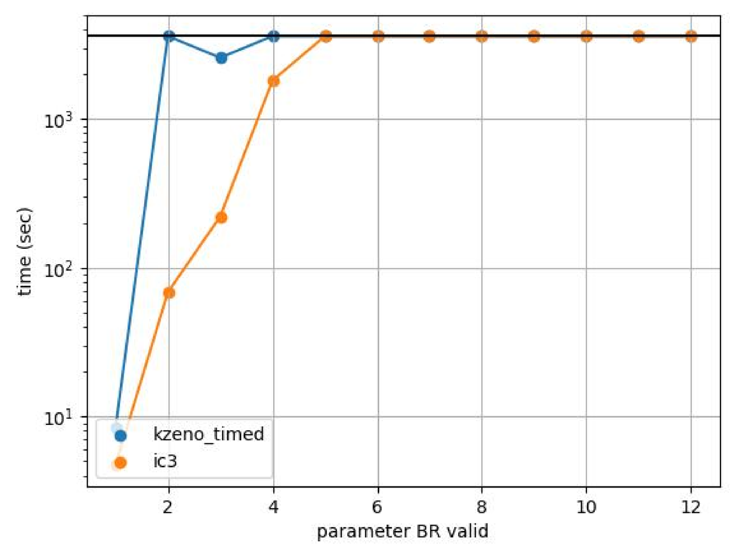
(a) λ evaluation



(b) ϵ evaluation



(c) Fischer experimental evaluation



(d) BR experimental evaluation

CONCLUSION

- We studied MTL with non-monotonic time.
- We defined MTLSK: a logic for systems with resettable skewed clocks.
- We implemented MTLSK symbolic model checking inside timed nuXmv[?].

Future works
- Study async composition with I/O components as in [1].
- Efficient techniques to find counter-examples using BMC as in [3].
- Case study with real life examples (e.g. 8N1 protocol).
- Relax assumptions on skewed clocks.
- Distributed runtime verification of MTLSK as in [7].

BIBLIOGRAPHY

[1] A. Bombardelli and S. Tonetta. Asynchronous Composition of Local Interface LTL Properties. In *NFM*, pages 508–526, 2022.

[2] A. Bombardelli and S. Tonetta. Reasoning with Metric Temporal Logic with Resettable Skewed Clocks. 2023. To appear, preproceding available at `https://es-static.fbk.eu/people/bombardelli/papers/nfm23/nfm23.pdf`.

[3] L. Bu, A. Cimatti, X. Li, S. Mover, and S. Tonetta. Model Checking of Hybrid Systems Using Shallow Synchronization. In *FMOODS/FORTE*, volume 6117 of *LNCS*, pages 155–169, 2010.

[4] A. Cimatti, A. Griggio, E. Magnago, M. Roveri, and S. Tonetta. Extending nuxmv with timed transition systems and timed temporal properties. In *Computer Aided Verification*, pages 376–386, Cham, 2019.

[5] A. Cimatti, A. Griggio, S. Mover, and S. Tonetta. IC3 Modulo Theories via Implicit Predicate Abstraction. In *TACAS*, volume 8413 of *Lecture Notes in Computer Science*, pages 46–61. Springer, 2014.

[6] A. Cimatti, A. Griggio, S. Mover, and S. Tonetta. Verifying LTL Properties of Hybrid Systems with K-Liveness. In A. Biere and R. Bloem, editors, *Computer Aided Verification*, pages 424–440, 2014.

[7] R. Ganguly, Y. Xue, A. Jonckheere, P. Ljungy, B. Schornsteiny, B. Bonakdarpour, and M. Herlihy. Distributed Runtime Verification of Metric Temporal Properties for Cross-Chain Protocols. *CoRR*, abs/2204.09796, 2022.