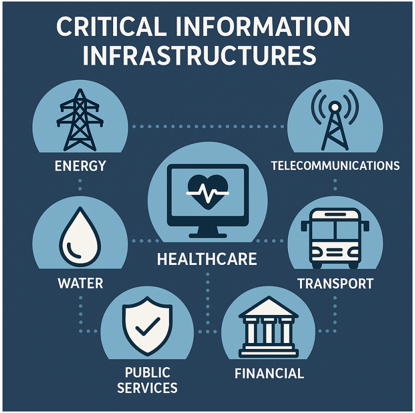
A Timed Predicate Temporal Logic Sequent Calculus

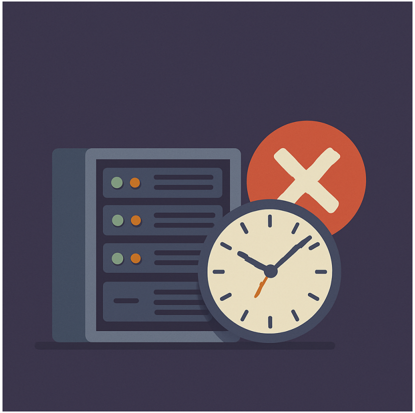
Javier Enriquez Mendoza

jww. Sam Speight and Vincent Rahli

Motivation and Background



Time properties



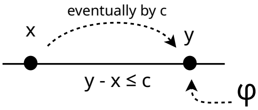
Temporal Logics

TPTL

TPTL is an extension of Linear Temporal Logic (LTL) & with explicit clock variables.

$$\varphi \quad ::= \quad p \mid \varphi \wedge \varphi \mid \neg\varphi \mid \varphi\, \mathbf{U}\, \varphi \mid \bigcirc\varphi \mid x \sim c \mid x \cdot \varphi$$

$$x \cdot \Diamond(x \leq c \wedge \varphi)$$



TPTL has been extended with past operators (TPTL + Past) **S** and **Y** .

Our Calculus

We present an extension of TPTL + Past

(1) Quantifiers: $\forall u : T.\varphi, \exists u : T.\varphi$
(2) General comparison operator: $t_1 \sim t_2$
(3) Discrete semantics based on timestamps t
(4) Formalized in Agda

Syntax

$$
\begin{array}{rcl}
\varphi & ::= & a \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \neg\varphi \mid \varphi \,\mathbf{U}\, \varphi \mid \bigcirc\varphi \mid \varphi \,\mathbf{S}\, \varphi \mid \mathbf{Y}\, \varphi \mid \\
 & & t \sim t \mid x \cdot \varphi \mid \forall u : T.\varphi \mid \exists u : T.\varphi \\
T & ::= & \mathbf{Agent} \mid \mathbf{Agents} \mid \mathbf{Data} \\
t & ::= & x \mid 0 \mid t \bullet t \mid \mathrm{s}(t) \\
\sim & ::= & < \mid = \\
a & ::= & p \mid \mathtt{send}(i, d, A) \mid \mathtt{recv}(i, d, j) \mid \mathtt{inter}(i, d)
\end{array}
$$

Semantics

Formulas are interpreted w.r.t.:

(1) t: a timestamp
(2) r: a function from timestamps to states
(3) π: an interpretation function
(4) v: a variable valuation

$$
\begin{array}{lcl}
\pi, r, t, v \models a & \iff & \pi(r(t))(a) \\
\pi, r, t, v \models \varphi \,\mathbf{U}\, \psi & \iff & \exists t' > t.(\pi, r, t', v \models \psi) \land \forall t'' \in [t, t').(\pi, r, t'', v \models \varphi) \\
\pi, r, t, v \models \bigcirc\varphi & \iff & \pi, r, t+1, v \models \varphi \\
\pi, r, t, v \models t_1 \sim t_2 & \iff & [\![t_1]\!]_v \sim [\![t_2]\!]_v \\
\pi, r, t, v \models x \cdot \varphi & \iff & \pi, r, t, v[x \mapsto t] \models \varphi \\
\pi, r, t, v \models \forall u : T.\varphi & \iff & \pi, r, t, v[u \mapsto z] \models \varphi \text{ for all } z \in [\![T]\!]
\end{array}
$$

Semantics

Formulas are interpreted w.r.t.:

(1) t: a timestamp
(2) r: a function from timestamps to states
(3) π: an interpretation function
(4) v: a variable valuation

$$
\begin{array}{lcl}
\pi, r, t, v \models a & \iff & \pi(r(t))(a) \\
\pi, r, t, v \models \varphi \,\mathbf{U}\, \psi & \iff & \exists t' > t.(\pi, r, t', v \models \psi) \wedge \forall t'' \in [t, t').(\pi, r, t'', v \models \varphi) \\
\pi, r, t, v \models \bigcirc\varphi & \iff & \pi, r, t+1, v \models \varphi \\
\pi, r, t, v \models t_1 \sim t_2 & \iff & [\![t_1]\!]_v \sim [\![t_2]\!]_v \\
\pi, r, t, v \models x \cdot \varphi & \iff & \pi, r, t, v[x \mapsto t] \models \varphi \\
\pi, r, t, v \models \forall u : T.\varphi & \iff & \pi, r, t, v[u \mapsto z] \models \varphi \text{ for all } z \in [\![T]\!]
\end{array}
$$

Semantics

Formulas are interpreted w.r.t.:

1. t: a timestamp
2. r: a function from timestamps to states
3. π: an interpretation function
4. v: a variable valuation

$$
\begin{aligned}
\pi, r, t, v &\models a && \iff && \pi(r(t))(a) \\
\pi, r, t, v &\models \varphi \,\mathbf{U}\, \psi && \iff && \exists t' > t.(\pi, r, t', v \models \psi) \land \forall t'' \in [t, t').(\pi, r, t'', v \models \varphi) \\
\pi, r, t, v &\models \bigcirc\varphi && \iff && \pi, r, t+1, v \models \varphi \\
\pi, r, t, v &\models t_1 \sim t_2 && \iff && [\![t_1]\!]_v \sim [\![t_2]\!]_v \\
\pi, r, t, v &\models x \cdot \varphi && \iff && \pi, r, t, v[x \mapsto t] \models \varphi \\
\pi, r, t, v &\models \forall u : T.\varphi && \iff && \pi, r, t, v[u \mapsto z] \models \varphi \text{ for all } z \in [\![T]\!]
\end{aligned}
$$

The Sequent Calculus

$\Gamma \vdash_{\mathsf{t}} \varphi$ states that φ holds at time t in the context Γ.

An hypothesis is of the form $(\psi)^r$, where r is a time annotation

$$\frac{\Gamma \vdash_{\mathsf{t}} \mathsf{t} < \mathsf{t}_1 \qquad \Gamma \vdash_{\mathsf{t}_1} \psi \qquad \Gamma, \mathsf{t} \leq x, x < \mathsf{t}_1 \vdash_x \varphi}{\Gamma \vdash_{\mathsf{t}} \varphi \, \mathbf{U} \, \psi} \ \mathbf{U}\,\mathsf{R}$$

$$\frac{\Gamma, \mathsf{t} < x, (\psi)^x, (\varphi)^{[\mathsf{t},x)} \vdash_{t_1} \gamma}{\Gamma, (\varphi \, \mathbf{U} \, \psi)^{\mathsf{t}} \vdash_{t_1} \gamma} \ \mathbf{U}\,\mathsf{L}$$

Expressiveness

Temporal operators such as "eventually" and "always" are defined as usual:

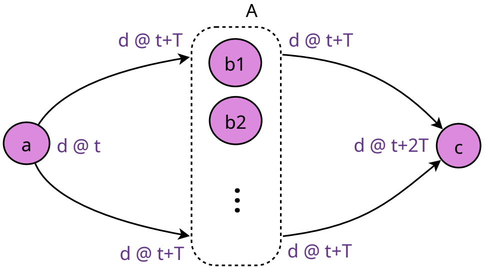
$$\Diamond\varphi := \texttt{true}\,\mathbf{U}\,\varphi \quad \text{and} \quad \Box\varphi := \neg\Diamond\neg\varphi$$

Time bounded version of the $\Diamond$ operator can now be defined:

$$\Diamond_t\varphi := x \cdot \Diamond(y \cdot y \leq x \bullet t \wedge \varphi)$$

Example

Assumptions:



$$\forall a : \textbf{Agent}.\forall d : \textbf{Data}.\forall A : \textbf{Agents}.\forall b : \textbf{Agent}.$$
$$\Box(\texttt{send}(a, d, A) \to \Diamond_T(b \in A \to \texttt{recv}(a, d, b)))$$

$$\forall a : \textbf{Agent}.\forall d : \textbf{Data}.\forall b : \textbf{Agent}.\forall c : \textbf{Agent}.$$
$$\Box(\texttt{recv}(a, d, b) \to \texttt{send}(b, d, \{c\}))$$

Conclusion:

$$\forall a : \textbf{Agent}.\forall d : \textbf{Data}.\forall b : \textbf{Agent}.\forall c : \textbf{Agent}.$$
$$\texttt{send}(a, d, \{b\}) \to \Diamond_{2T}(\texttt{recv}(b, d, c))$$

Takeaways

A timed predicate temporal logic

$$\Diamond_t \varphi := x \cdot \Diamond(y \cdot y \leq x \bullet t \land \varphi)$$

A labeled sequent calculus

$$\frac{\Gamma, \mathsf{t} < x, (\psi)^{x}, (\varphi)^{[\mathsf{t},x)} \vdash_{t_1} \gamma}{\Gamma, (\varphi \,\mathbf{U}\, \psi)^{\mathsf{t}} \vdash_{t_1} \gamma} \;\mathbf{U}\,\mathsf{L}$$

Discrete semantics

$$\pi, r, t, v \models x \cdot \varphi \iff \pi, r, t, v[x \mapsto t] \models \varphi$$

Application to distributed systems

$$\forall a : \mathbf{Agent}. \forall d : \mathbf{Data}. \forall b : \mathbf{Agent}. \forall c : \mathbf{Agent}.$$
$$\mathtt{send}(a, d, \{b\}) \to \Diamond_{2T}(\mathtt{recv}(b, d, c))$$

Future work: type system

Takeaways

A timed predicate temporal logic

$$\Diamond_t \varphi := x \cdot \Diamond(y \cdot y \leq x \bullet t \wedge \varphi)$$

Discrete semantics

$$\pi, r, t, v \models x \cdot \varphi \iff \pi, r, t, v[x \mapsto t] \models \varphi$$

A labeled sequent calculus

$$\frac{\Gamma, \mathsf{t} < x, (\psi)^{x}, (\varphi)^{[\mathsf{t}, x)} \vdash_{t_1} \gamma}{\Gamma, (\varphi \,\mathbf{U}\, \psi)^{\mathsf{t}} \vdash_{t_1} \gamma} \ \mathbf{U}\,\mathsf{L}$$

Application to distributed systems

$$\forall a : \textbf{Agent}. \forall d : \textbf{Data}. \forall b : \textbf{Agent}. \forall c : \textbf{Agent}.$$
$$\texttt{send}(a, d, \{b\}) \rightarrow \Diamond_{2T}(\texttt{recv}(b, d, c))$$

Future work: type system