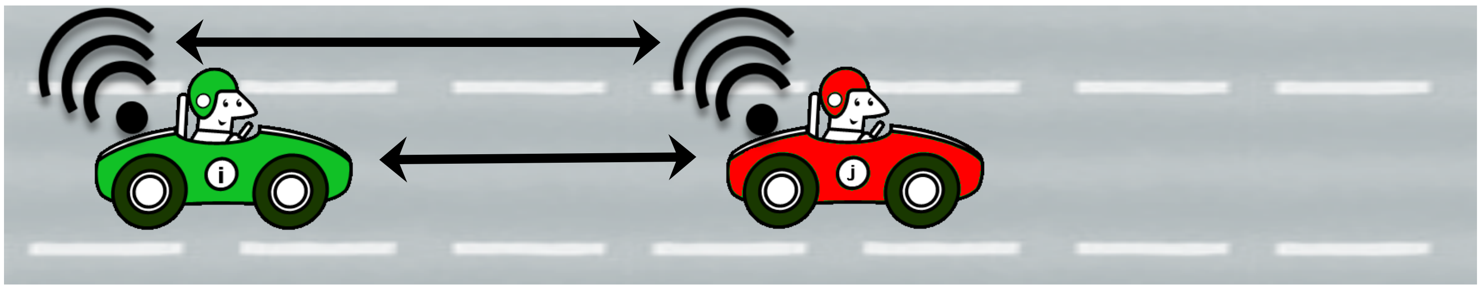
Efficiency Analysis of Formally Verified Adaptive Cruise Controllers

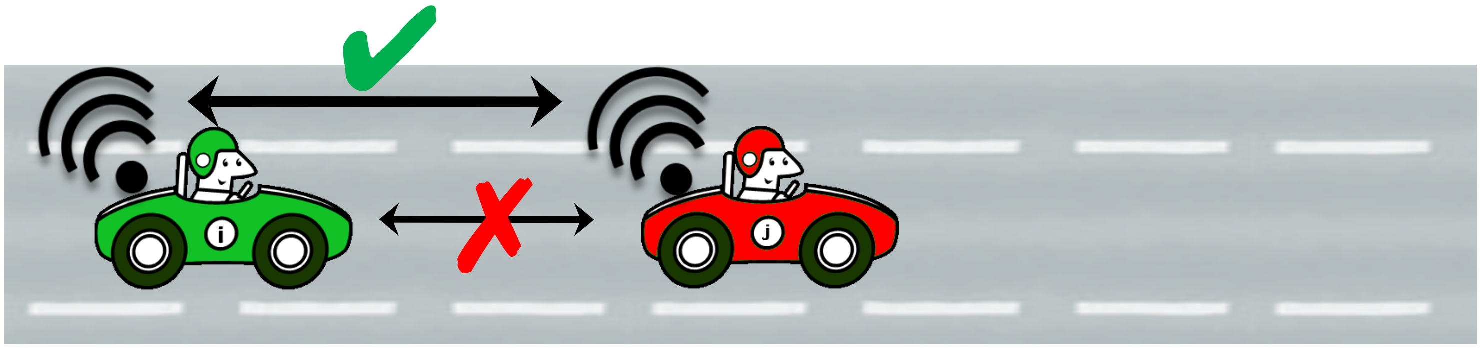
Sarah M. Loos, David Witmer, Peter Steenkiste, and André Platzer
Computer Science Department, Carnegie Mellon University

ITSC 2013

Motivation: Adaptive Cruise Control

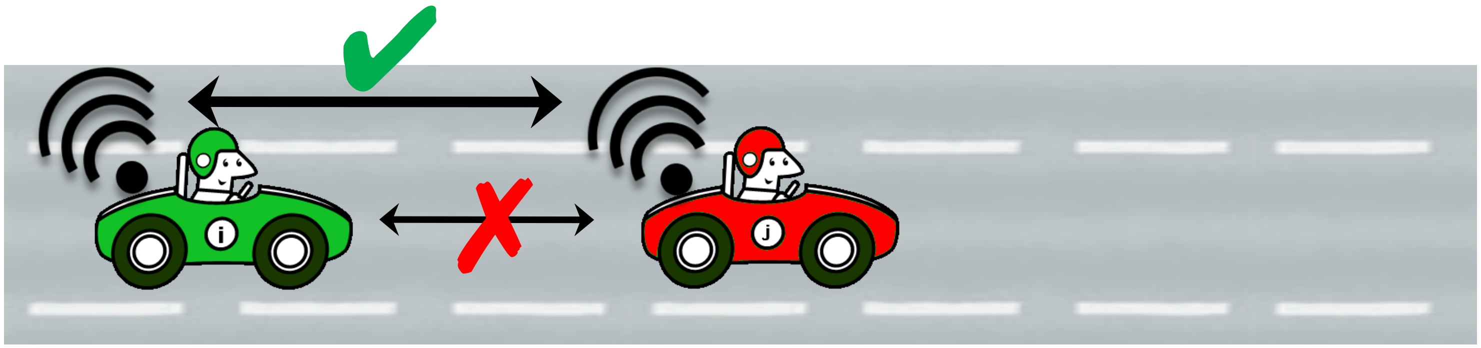


Motivation: Adaptive Cruise Control

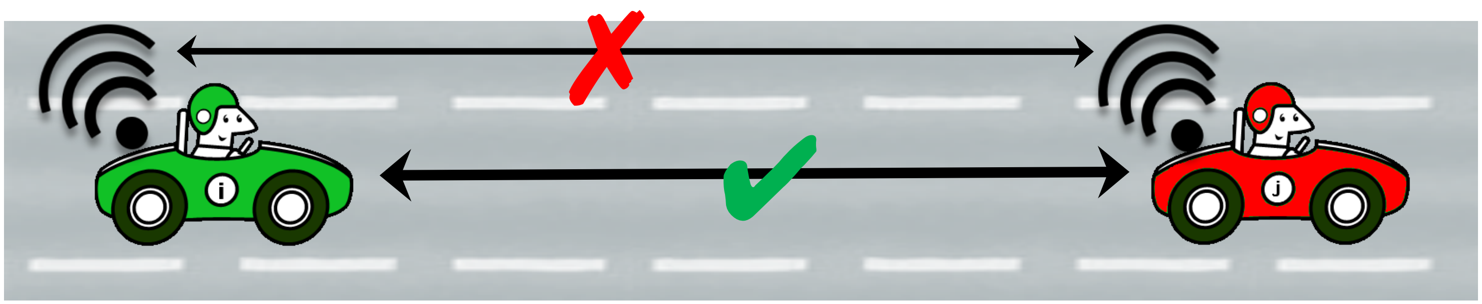


Low packet loss, small margin for error.

Motivation: Adaptive Cruise Control

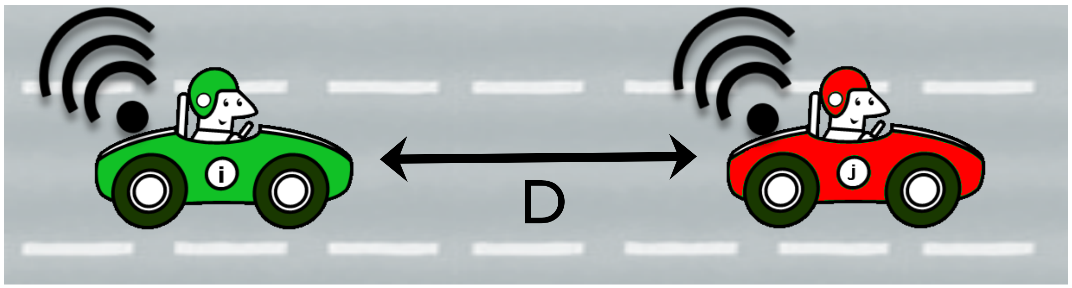


Low packet loss, small margin for error.



High packet loss, large margin for error.

Adaptive Cruise Control



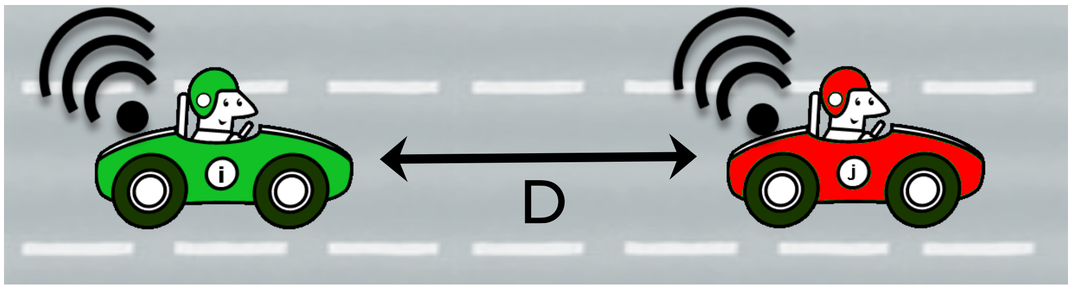
$< x_f, v_f >$ $< x_l, v_l >$

A = max acceleration
-B = max braking
$\mathcal{T}$ = timeout

When the follower receives an update from the leader about its position and velocity, the follow car chooses a new safe acceleration.

If no message is received within timeout $\mathcal{T}$, the car may brake or a human driver may take control of the vehicle.

Adaptive Cruise Control



$< x_f, v_f >$ $< x_l, v_l >$

A = max acceleration
$-B$ = max braking
$\mathcal{T}$ = timeout

When the follower receives an update from the leader about its position and velocity, the follow car chooses a new safe acceleration.

If no message is received within timeout $\mathcal{T}$, the car may brake or a human driver may take control of the vehicle.

Maximum Acceleration Choice

$$a_f(v_f, v_l, D, \mathcal{T}) = \begin{cases} A & \text{if } a1 \geq A \\ 0 & \text{if } v_f = 0 \wedge a1 \geq 0 \\ a2 & \text{if } a1 < \frac{-v_f}{\mathcal{T}} \wedge -B \leq a2 \\ a1 & \text{if } a1 >= \frac{-v_f}{\mathcal{T}} \wedge -B \leq a1 \\ -B & \text{o.w.} \end{cases}$$

$$a1 := \frac{\sqrt{B^2\mathcal{T}^2 - 4Bv_f\mathcal{T} + 8BD + 4v_l^2} - B\mathcal{T} - 2v_f}{2\mathcal{T}}$$

$$a2 := \frac{-v_f^2}{2(D + \frac{v_l^2}{2B})}$$

Formal Verification of Safety

$$\begin{aligned}
\texttt{ACC} &\equiv (ctrl; dyn)^* \\
ctrl &\equiv \ell_{ctrl} \mid\mid f_{ctrl}; \\
\ell_{ctrl} &\equiv (a_\ell := *; \quad ?(-B \leq a_\ell \leq A)) \\
f_{ctrl} &\equiv a_f := a_f(v_f, v_l, D, \mathcal{T}) \\
D &\equiv x_l - x_f \\
dyn &\equiv (t := 0; \; t' = 1, \\
&\quad x'_f = v_f, \; v'_f = a_f, \\
&\quad x'_\ell = v_\ell, \; v'_\ell = a_\ell \\
&\quad \& \; v_f \geq 0 \; \wedge \; v_\ell \geq 0 \; \wedge \; t \leq \mathcal{T})
\end{aligned}$$

Formal Verification of Safety

initial condition $\rightarrow$ [model] (safety)

$$
\begin{aligned}
\texttt{ACC} &\equiv (ctrl; dyn)^* \\
ctrl &\equiv \ell_{ctrl} \;||\; f_{ctrl}; \\
\ell_{ctrl} &\equiv (a_\ell := *; \quad ?(-B \le a_\ell \le A)) \\
f_{ctrl} &\equiv a_f := a_f(v_f, v_l, D, \mathcal{T}) \\
D &\equiv x_l - x_f \\
dyn &\equiv (t := 0;\ t' = 1, \\
&\qquad x'_f = v_f,\ v'_f = a_f, \\
&\qquad x'_\ell = v_\ell,\ v'_\ell = a_\ell \\
&\qquad \&\ v_f \ge 0 \ \wedge\ v_\ell \ge 0 \ \wedge\ t \le \mathcal{T})
\end{aligned}
$$

Formal Verification of Safety

$$(x_f \le x_l \wedge v_f^2 \le v_l^2 + 2DB) \to [\mathtt{ACC}](x_f \le x_l)$$

$$\begin{aligned}
\mathtt{ACC} &\equiv (ctrl; dyn)^* \\
ctrl &\equiv \ell_{ctrl} \;||\; f_{ctrl}; \\
\ell_{ctrl} &\equiv (a_\ell := *; \quad ?(-B \le a_\ell \le A)) \\
f_{ctrl} &\equiv a_f := a_f(v_f, v_l, D, \mathcal{T}) \\
D &\equiv x_l - x_f \\
dyn &\equiv (t := 0; \; t' = 1, \\
&\qquad x_f' = v_f, \; v_f' = a_f, \\
&\qquad x_\ell' = v_\ell, \; v_\ell' = a_\ell \\
&\qquad \& \; v_f \ge 0 \;\wedge\; v_\ell \ge 0 \;\wedge\; t \le \mathcal{T})
\end{aligned}$$

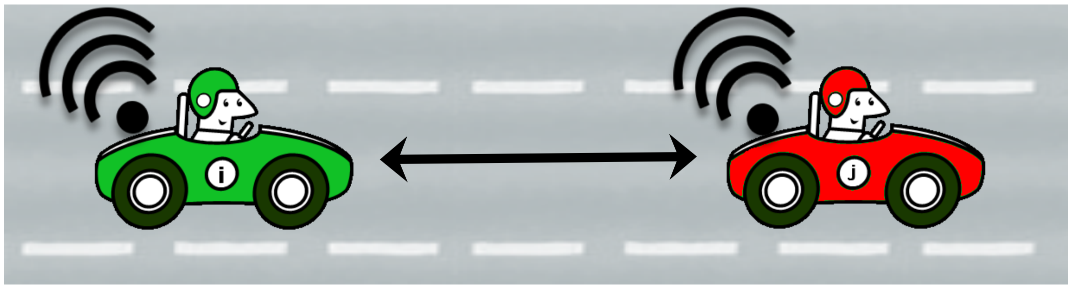
Formal Verification of Safety

$$(x_f \leq x_l \wedge v_f^2 \leq v_l^2 + 2DB) \rightarrow [\texttt{ACC}](x_f \leq x_l)$$

$$\begin{aligned}
\texttt{ACC} &\equiv (ctrl; dyn)^* \\
ctrl &\equiv \ell_{ctrl} \mid\mid f_{ctrl}; \\
\ell_{ctrl} &\equiv (a_\ell := *;\ \ ?(-B \leq a_\ell \leq A)) \\
f_{ctrl} &\equiv a_f := a_f(v_f, v_l, D, \mathcal{T}) \\
D &\equiv x_l - x_f \\
dyn &\equiv (t := 0;\ t' = 1, \\
&\quad\ x_f' = v_f,\ v_f' = a_f, \\
&\quad\ x_\ell' = v_\ell,\ v_\ell' = a_\ell \\
&\quad\ \&\ v_f \geq 0\ \wedge\ v_\ell \geq 0\ \wedge\ t \leq \mathcal{T})
\end{aligned}$$

✔ Verified in KeYmaera

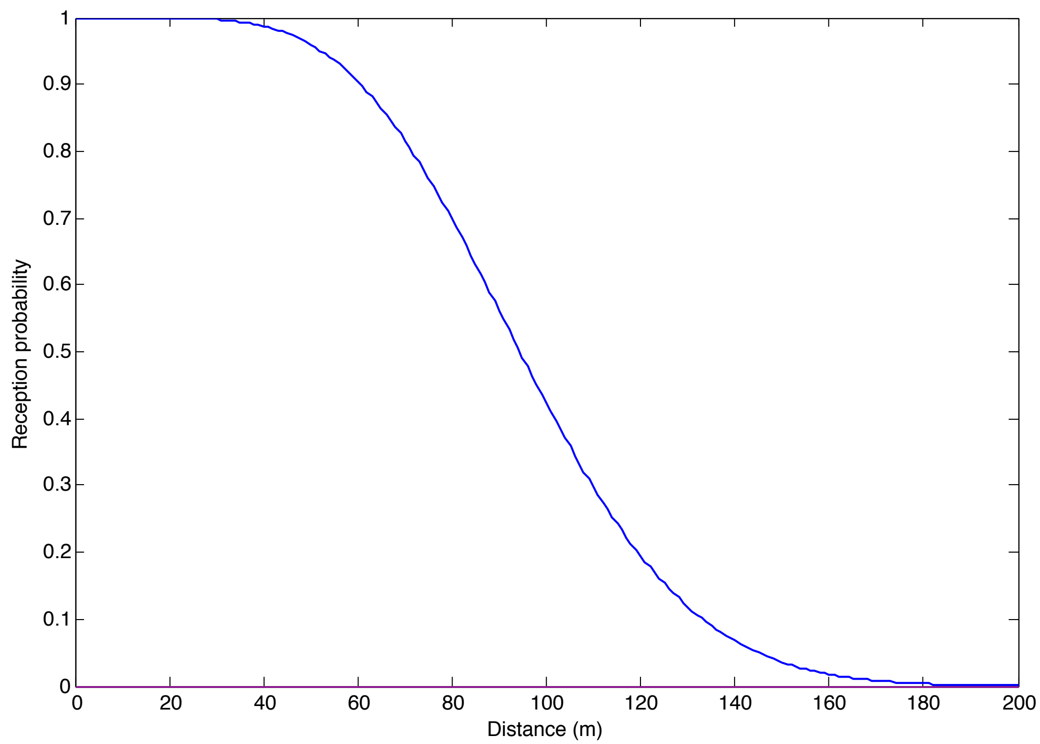
V2V Overview



- Using 802.11p standard
- Cars transmit current position and velocity
- Transmission frequency of 10Hz for safety-critical systems
- Assume 100 meter transmission power.

Signal Strength

The **Nakagami Fading Model** gives us the probability of receiving a single packet as a function of distance. We assume 100 meter transmission power ψ



$$p(D,\psi) = e^{-3\frac{D^2}{\psi^2}}\left(1 + 3\frac{D^2}{\psi^2} + \frac{9}{2}\frac{D^4}{\psi^4}\right)$$

Choosing the Timeout

Average acceleration choice over state-space for a given timeout $\mathcal{T}$:

$$\text{Eff}_{a_f}(\mathcal{T}) = \frac{1}{S}\iiint a_f(v_f, v_l, D, \mathcal{T})\ dD\ dv_l\ dv_f$$

Average probability of requiring driver assistance for a given timeout $\mathcal{T}$:

$$\text{Eff}_{assist}(\mathcal{T}) = \frac{1}{S}\iiint Pr(t <= \mathcal{T})\ dD\ dv_l\ dv_f$$

$$Pr(t <= \mathcal{T}) = 1 - (1 - p(D))^{\lfloor \text{freq} * \mathcal{T} \rfloor}$$

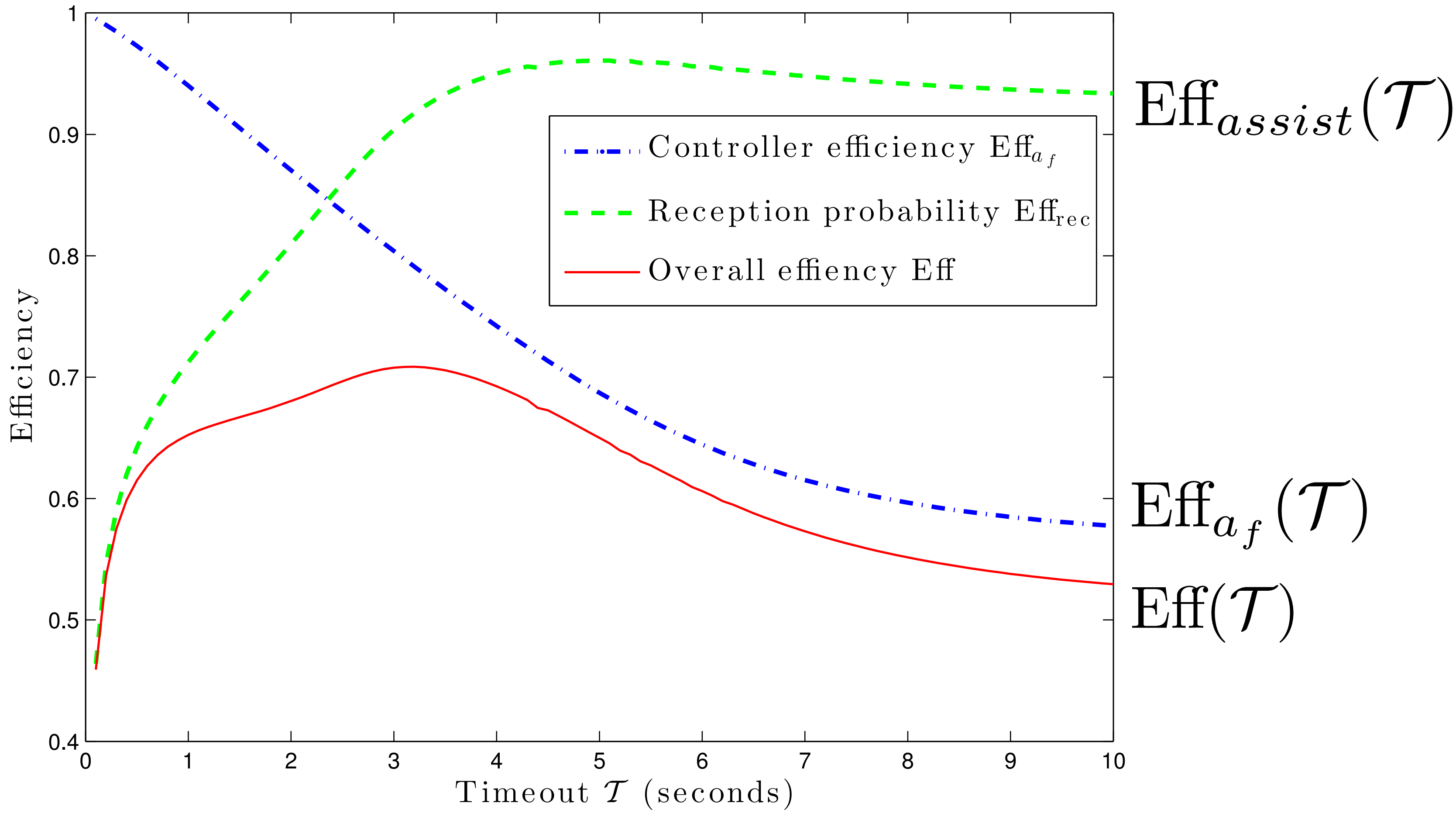
Choosing the Timeout

Average expected acceleration choice over state-space for a given timeout $\mathcal{T}$:

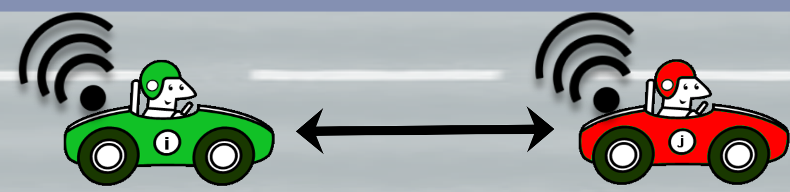
$$\mathrm{Eff}(\mathcal{T}) = \frac{1}{S} \iiint \underbrace{a_f(v_f, v_l, D, \mathcal{T})}_{\text{Control function for follower's acceleration}} * \underbrace{Pr(t <= \mathcal{T})}_{\text{Probability update received within timeout at distance D}} \, dD \; dv_l \; dv_f$$

Normalization for size of analyzed state space

Efficiency Analysis of ACC



Conclusions

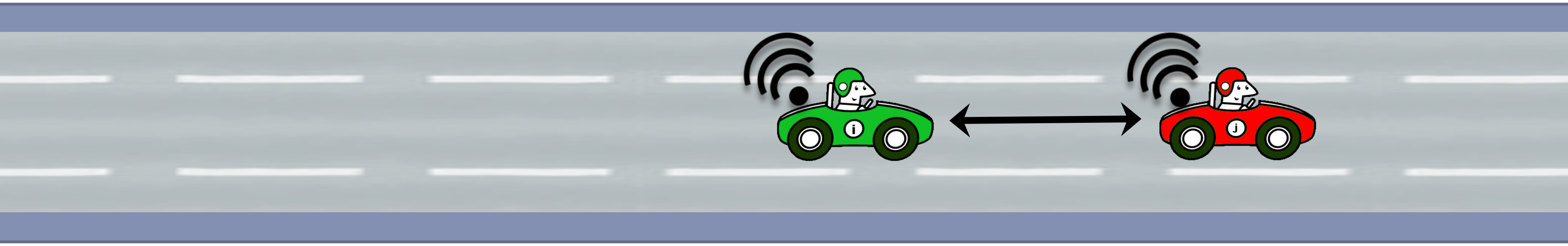


Challenges

- Infinite, continuous, and evolving state space, $\mathbf{R}^{\infty}$
- Continuous dynamics
- Discrete control decisions
- Require a symbolic controller which is both safe and efficient
- Probabilistic message passing
- Efficiency is ill-defined

Solutions

- Use of Differential Dynamic Logic (dL) ensures safety in *all* states
- Proof in dL also provides symbolic controllers, which allow for natural tradeoff analysis
- By quantifying the tradeoff between efficiency and timeout we discover an optimal choice
- Punish timeout failure as maximum braking



Thank You!