Towards Formal Verification of Freeway Traffic Control

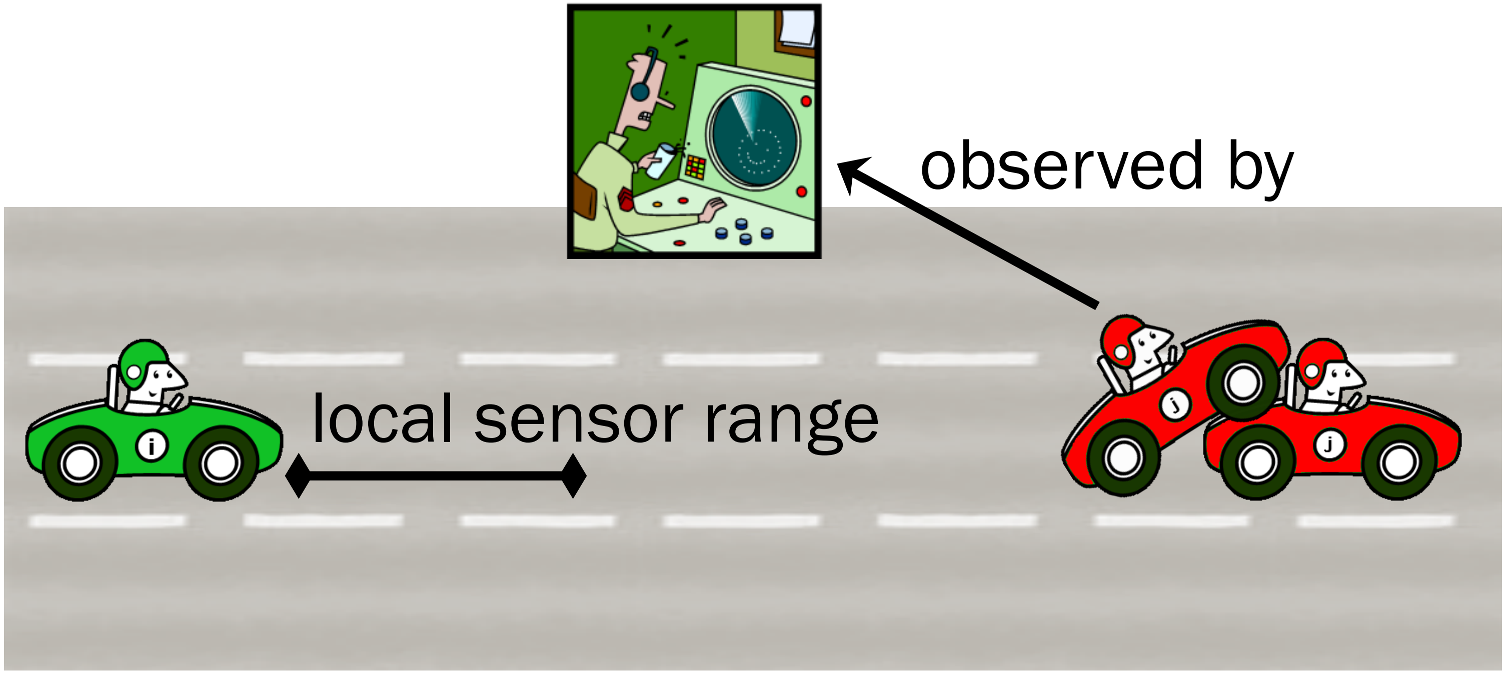
Stefan Mitsch
Information Systems Group
Johannes Kepler University

Sarah Loos, and André Platzer
Computer Science Department
Carnegie Mellon University

April 19, 2012

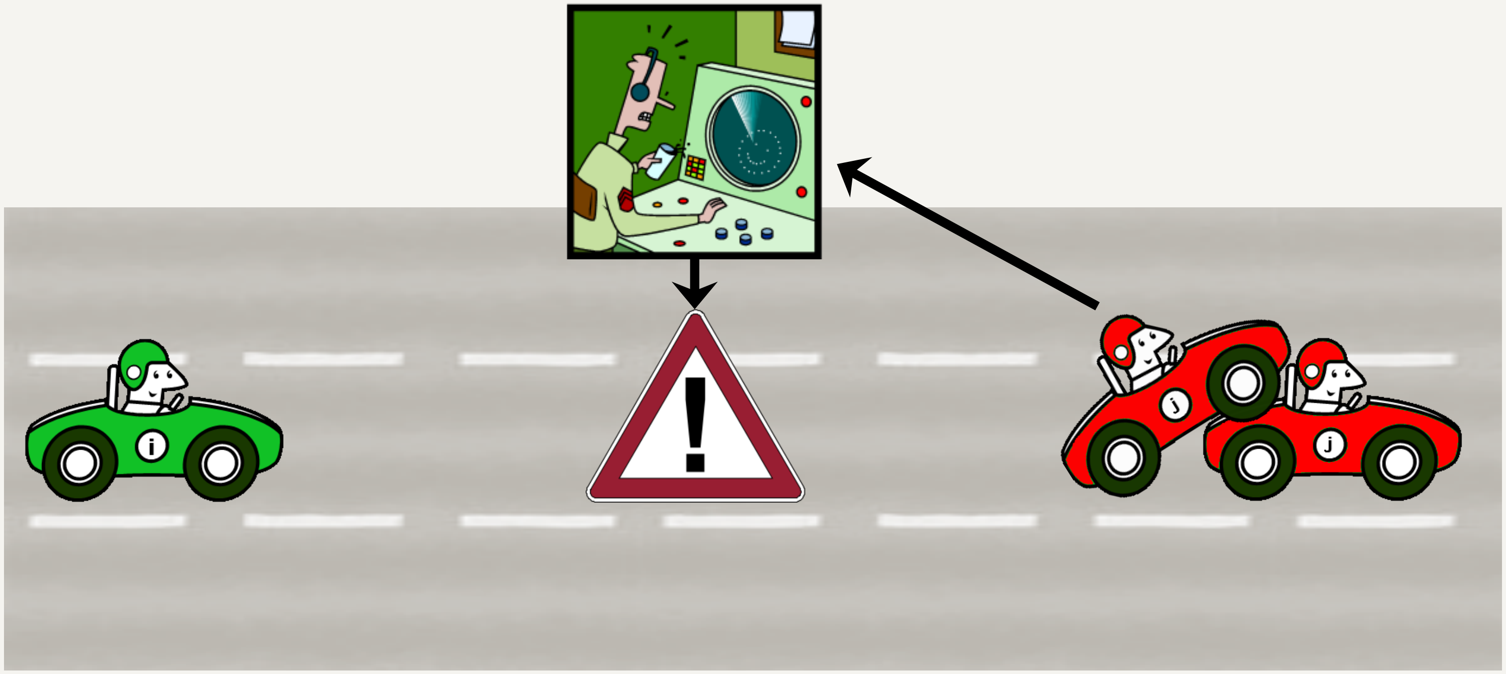
How Can We Prove Complex Highways?

How Can We Prove Complex Highways?



Traffic centers aim at global functioning and safety.

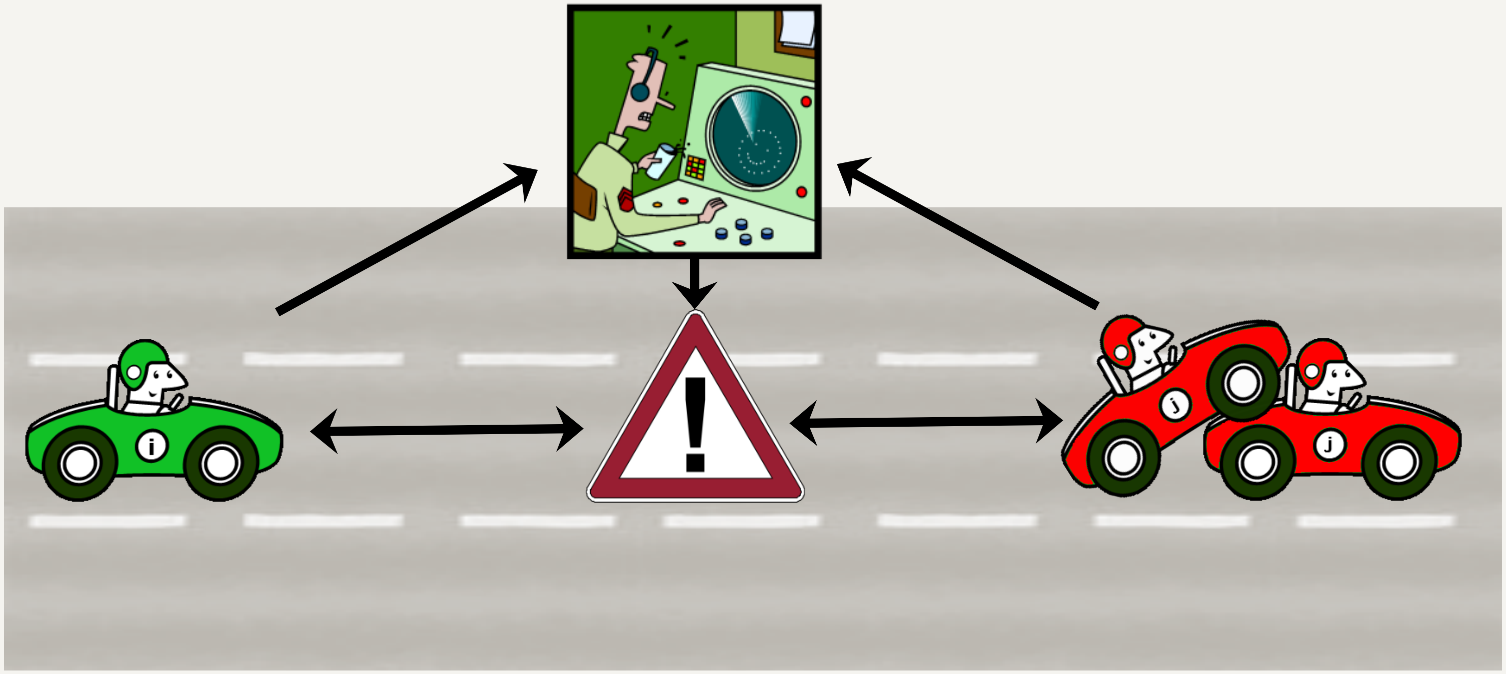
How Can We Prove Complex Highways?



Traffic centers aim at global functioning and safety.

Open-loop control systems (give advice, e.g., speed limits)

How Can We Prove Complex Highways?



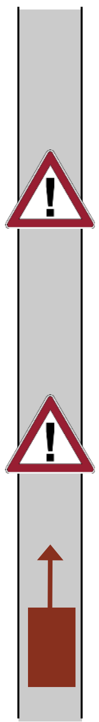
Traffic centers aim at global functioning and safety.

Open-loop control systems (give advice, e.g., speed limits)

Closed-loop: use car information and feed advice as set values into car controllers

Traffic Control: Outline

Variable Speed
Limit Control



1 vehicle
n traffic advice

Moving Incident
Warning Control

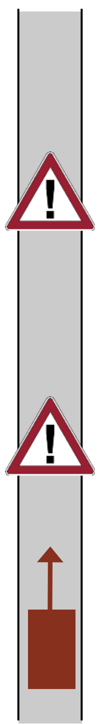
1 vehicle
1 incident
n traffic advice

Moving Incident
Warning Control
w/ Zeno Avoidance

1 vehicles
1 incident
n traffic advice, 1 warning

Traffic Control: Variable Speed Limit

Variable Speed
Limit Control



1 vehicle
n traffic advice

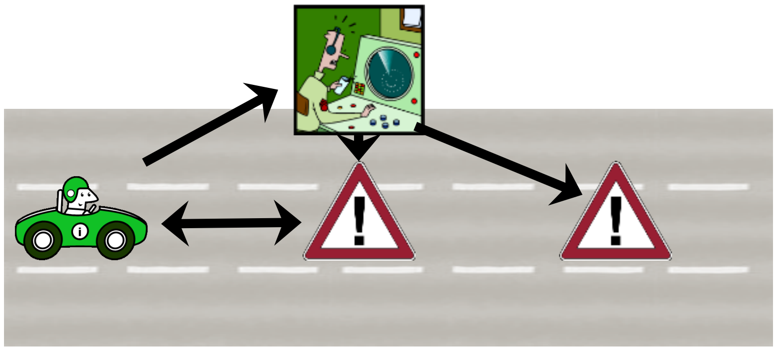
Moving Incident
Warning Control

1 vehicle
1 incident
n traffic advice

Moving Incident
Warning Control
w/ Zeno Avoidance

1 vehicles
1 incident
n traffic advice, 1 warning

Variable Speed Limit Challenges



Traffic center: intelligent speed adaptation system

- **Global decisions** beyond local sensor range
- **Multiple**, sequentially issued **speed limits**

In-car driver assistance systems: traffic sign detection

- Find **design parameters** (camera resolution, etc.)

Differential Dynamic Logic*

*The short version.

Initial Conditions → [Model] Requirements

Differential Dynamic Logic

$$\text{Initial Conditions} \rightarrow [\text{Model}]\ \text{Requirements}$$

Differential Dynamic Logic

$$\underbrace{\text{Initial Conditions}}_{\text{logical formula}} \rightarrow [\text{Model}]\ \underbrace{\text{Requirements}}_{\text{logical formula}}$$

Differential Dynamic Logic

$$\underbrace{v_c \leq v_{sl}}_{\text{logical formula}} \rightarrow [\text{Model}] \; \underbrace{v_c \leq v_{sl}}_{\text{logical formula}}$$

Differential Dynamic Logic

$$\underbrace{v_c \leq v_{sl}}_{\text{logical formula}} \rightarrow [\textcolor{red}{\text{Model}}]\ \underbrace{v_c \leq v_{sl}}_{\text{logical formula}}$$

Differential Dynamic Logic

$$\underbrace{v_c \le v_{sl}}_{\text{logical formula}} \rightarrow \underbrace{[\textcolor{red}{\text{Model}}]}_{\text{hybrid program}} \; \underbrace{v_c \le v_{sl}}_{\text{logical formula}}$$

Differential Dynamic Logic

$$\underbrace{v_c \le v_{sl}}_{\text{logical formula}} \to [\overbrace{\underbrace{\color{red}{\text{Model}}}_{\text{hybrid program}}}^{\text{discrete control} \quad \text{continuous dynamics}}] \underbrace{v_c \le v_{sl}}_{\text{logical formula}}$$

Differential Dynamic Logic

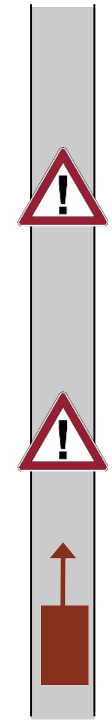
$$\underbrace{v_c \le v_{sl}}_{\text{logical formula}} \;\to\; [\underbrace{(\overbrace{\text{ctrl}}^{\text{discrete control}};\overbrace{\text{dyn}}^{\text{continuous dynamics}})^*}_{\text{hybrid program}}]\;\; \underbrace{v_c \le v_{sl}}_{\text{logical formula}}$$

Differential Dynamic Logic

$$\underbrace{v_c \le v_{sl}}_{\text{logical formula}} \to \underbrace{[(\overbrace{\text{ctrl}}^{\text{discrete control}};\ \overbrace{x' = v;\ v' = a}^{\text{continuous dynamics}})^*]}_{\text{hybrid program}}\, \underbrace{v_c \le v_{sl}}_{\text{logical formula}}$$

Traffic Control: Speed Limit Compliance

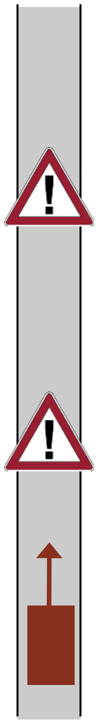
Car c is able to follow
a speed limit advice sl if $c \searrow sl$



Traffic Control: Speed Limit Compliance

Car c is able to follow
a speed limit advice sl if $c \searrow sl$

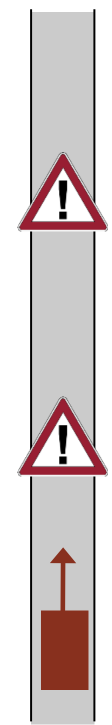
$$c \searrow sl \equiv \left(v_c \leq v_{sl} \vee x_{sl} \geq x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b} \right) \wedge v_c \geq 0 \wedge v_{sl} \geq 0$$



Traffic Control: Speed Limit Compliance

Car c is able to follow
a speed limit advice sl if $c \searrow sl$

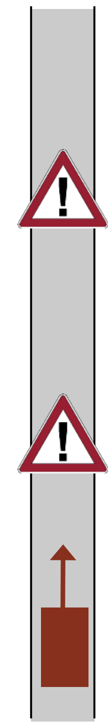
$$c \searrow sl \equiv \left(\underbrace{v_c \leq v_{sl}}_{\text{car already follows speed limit advice}} \vee x_{sl} \geq x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b} \right) \wedge v_c \geq 0 \wedge v_{sl} \geq 0$$



Traffic Control: Speed Limit Compliance

Car c is able to follow
a speed limit advice sl if $c \searrow sl$

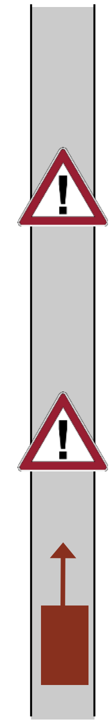
$$c \searrow sl \equiv \left(\underbrace{v_c \leq v_{sl}}_{\text{car already follows speed limit advice}} \lor \underbrace{x_{sl} \geq x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b}}_{\text{car is still able to brake}} \right) \land v_c \geq 0 \land v_{sl} \geq 0$$



Traffic Control: Speed Limit Compliance

To Prove: $(c \searrow sl) \rightarrow [vsl](x_c \geq x_{sl} \rightarrow v_c \leq v_{sl})$

$$\begin{aligned}
vsl &\equiv (ctrl; dyn)^* \\
ctrl &\equiv ctrl_{car} || ctrl_{ctr} \\
ctrl_{car} &\equiv (a_c := -b) \\
&\quad \cup \left(?Safe_{\underline{x_{sl}}};\ a_c := *;\ ?(-b \leq a_c \leq A)\right) \\
&\quad \cup \left(?x_c \geq x_{sl};\ a_c := *; ?(-b \leq a_c \leq A \wedge \boxed{a_c \leq \frac{v_{sl} - v_c}{\varepsilon}})\right) \\
&\quad \cup (?v_c = 0;\ a_c := 0) \\
Safe_{\underline{sl}} &\equiv \boxed{x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b} + \left(\frac{A}{b} + 1\right) \cdot \left(\frac{A}{2} \cdot \varepsilon^2 + \varepsilon \cdot v_c\right) \leq x_{sl}} \\
ctrl_{ctr} &\equiv (x_{sl} := x_{sl};\ v_{sl} := v_{sl}) \\
&\quad \cup \left(x_{sl} := *;\ v_{sl} := *; ?(v_{sl} \geq 0 \wedge Safe_{\underline{sl}})\right) \\
dyn &\equiv (t := 0;\ x_c' = v_c, v_c' = a_c, t' = 1 \\
&\qquad \& \ v_c \geq 0 \wedge t \leq \varepsilon)
\end{aligned}$$



Initial Conditions → [Model] Requirements

Traffic Control: Speed Limit Compliance

To Prove: $(c \searrow sl) \rightarrow [vsl](x_c \geq x_{sl} \rightarrow v_c \leq v_{sl})$

✔ Verified in KeYmaera

$$vsl \equiv (ctrl; dyn)^*$$

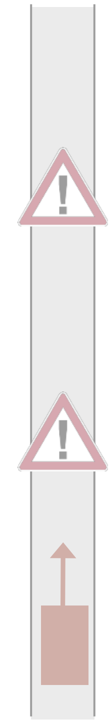
$$ctrl \equiv ctrl_{car} \| ctrl_{ctr}$$

$$\begin{aligned}
ctrl_{car} \equiv\ & (a_c := -b) \\
& \cup (?Safe_{\underline{x_{sl}}};\ a_c := *;\ ?(-b \leq a_c \leq A)) \\
& \cup (?x_c \geq x_{sl};\ a_c := *; ?(-b \leq a_c \leq A \wedge a_c \leq \frac{v_{sl} - v_c}{\varepsilon})) \\
& \cup (?v_c = 0;\ a_c := 0)
\end{aligned}$$

$$Safe_{\underline{sl}} \equiv x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b} + \left(\frac{A}{b} + 1\right) \cdot \left(\frac{A}{2} \cdot \varepsilon^2 + \varepsilon \cdot v_c\right) \leq x_{sl}$$

$$\begin{aligned}
ctrl_{ctr} \equiv\ & (x_{sl} := x_{sl};\ v_{sl} := v_{sl}) \\
& \cup (x_{sl} := *;\ v_{sl} := *; ?(v_{sl} \geq 0 \wedge Safe_{\underline{sl}}))
\end{aligned}$$

$$\begin{aligned}
dyn \equiv\ & (t := 0;\ x_c' = v_c, v_c' = a_c, t' = 1 \\
& \&\ v_c \geq 0 \wedge t \leq \varepsilon)
\end{aligned}$$



Initial Conditions → [Model] Requirements

Design Implications (Traffic center)

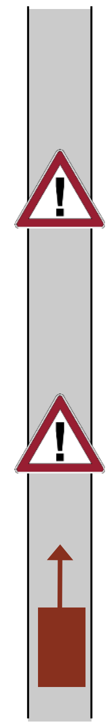
$$Safe_{\underline{sl}} \equiv \boxed{x_c} + \frac{\boxed{v_c^2} - v_{sl}^2}{2 \cdot \boxed{b}} + \left(\boxed{\frac{A}{b}} + 1\right) \cdot \left(\boxed{\frac{A}{2}} \cdot \varepsilon^2 + \varepsilon \cdot v_c\right) \le x_{sl}$$

Traffic center must be able to **measure** or **estimate car parameters**

- Position, current velocity
- Maximum acceleration, braking power

Communication delay must be **bounded**

- May not be possible with wireless communication: fault-tolerant design



Design Implications (Driver assistance 1/2)

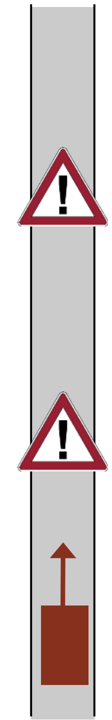
$$Safe_{\underline{sl}} \equiv x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b} + \left(\frac{A}{b} + 1\right) \cdot \left(\frac{A}{2} \cdot \varepsilon^2 + \varepsilon \cdot v_c\right) \leq x_{sl}$$

Image size

- Adjust 60km/h to 50km/h speed limit
  braking at 2m/s² takes 26m braking distance
- Camera features: $res = \dfrac{w_{image} \cdot l_{focal}}{d \cdot w_{chip}}$
- Speed limit sign: width = 12 pixels

Image processing tradeoff

(higher resolution vs. processing speed)



[1] D. Deguchi, M. Shirasuna, K. Doman, I. Ide, and H. Murase *(2011)*

Design Implications (Driver assistance 2/2)

$$Safe_{\underline{sl}} \equiv x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b} + \left(\frac{A}{b} + 1\right) \cdot \left(\frac{A}{2} \cdot \varepsilon^2 + \varepsilon \cdot v_c\right) \leq x_{sl}$$

Image processing tradeoff

Requirement: 20px width

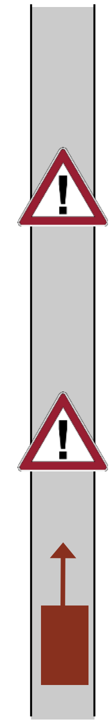
(a) Replace 63mm **lens** with 102mm

(b) **Increase algorithm performance**

1040px instead of 640px image

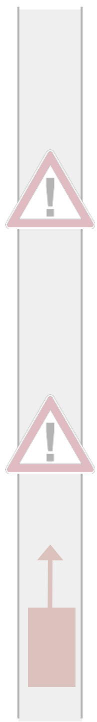
(c) Keep lens/camera, but **brake harder**

braking at 3.4m/s² instead of 2m/s² gives braking distance of 16m



Traffic Control: Incident Warning

Variable Speed
Limit Control



1 vehicle
n traffic advice

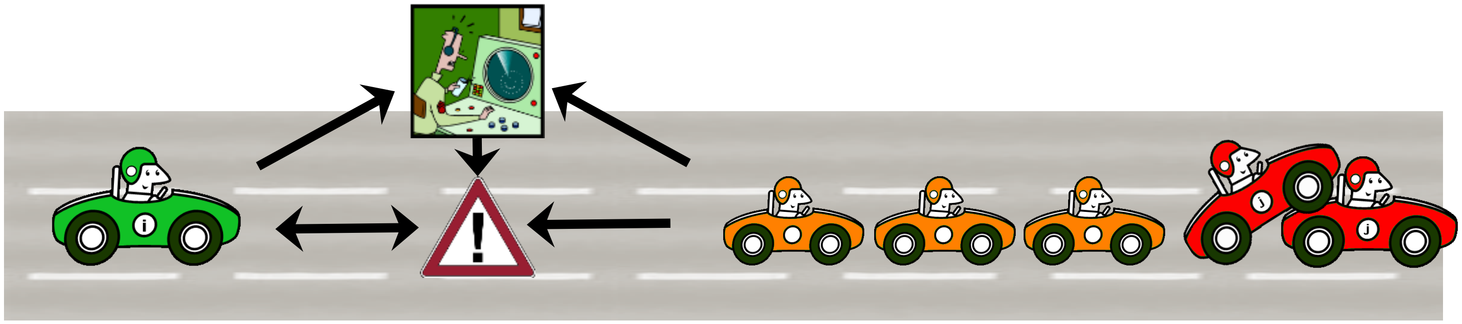
Moving Incident
Warning Control

1 vehicle
1 incident
n traffic advice/warnings

Moving Incident
Warning Control
w/ Zeno Avoidance

1 vehicles
1 incident
n traffic advice, 1 warning

Incident Warning Challenges



Traffic center: long-term incident warning
(e.g., accidents, traffic jams, wrong-way drivers)

- Motion **towards** car
- May **exceed local sensor coverage**

In-car driver assistance systems: short-term

- Find **design parameters** (camera resolution, etc.)
- Estimate system **performance** (e.g., speed reduction)

Traffic Control: Incident Warning

Car c is able to react to an incident warning sl if $(c \to\!\boxdot\, sl)$

Traffic Control: Incident Warning

Car c is able to react to an incident warning sl if $(c \rightarrow\!\boxdot\ sl)$

$$(c \rightarrow\!\boxdot\ sl) \equiv (\underbrace{x_{sl} \geq x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b} \vee v_c \leq v_{sl}}_{\text{As before: speed limit compliance}}) \wedge (\underbrace{c \,\square\, sl \vee c \boxdot sl}_{\text{Requirements inside or outside warning area}})$$

Traffic Control: Incident Warning

Car c is able to react to an incident warning sl if $(c \rightarrow\!\boxdot\; sl)$

$$(c \rightarrow\!\boxdot\; sl) \equiv \left(x_{sl} \geq x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b} \vee v_c \leq v_{sl}\right) \wedge \left(c \Box\, sl \vee c \boxdot\, sl\right)$$

Outside warning area

$$(c \Box\, sl) \equiv \underbrace{x_c + \frac{v_c^2 - v_{min}^2}{2 \cdot b} \cdot \left(1 + \frac{v_i}{v_{min}}\right) < x_i - D}_{\text{Car can still brake before warning area, keeping in mind that incident may move towards car}} \vee \underbrace{x_c > x_i}_{\text{After incident}}$$

Traffic Control: Incident Warning

Car c is able to react to an incident warning sl if $(c \rightarrow\boxdot\, sl)$

$$(c \rightarrow\boxdot\, sl) \equiv \left(x_{sl} \geq x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b} \vee v_c \leq v_{sl}\right) \wedge \left(c \Box sl \vee c \boxdot sl\right)$$

$$c \Box sl \equiv x_c + \frac{v_c^2 - v_{min}^2}{2 \cdot b} \cdot \left(1 + \frac{v_i}{v_{min}}\right) < x_i - D \vee x_c > x_i$$

Inside warning area

$$c \boxdot sl \equiv \left(\underbrace{x_{sl} \leq x_i}_{\text{Warning is in front of incident}} \wedge \underbrace{(x_{sl} - x_c) \cdot v_i \leq (x_i - x_{sl}) \cdot v_{min}}_{\text{Car will reach warning faster than incident}}\right) \vee \underbrace{x_c \geq x_{sl}}_{\text{Car already passed warning}}$$

Traffic Control: Incident Warning

To Prove:

$$c \rightarrow\!\boxdot\ sl \rightarrow [vsli]\Big(\big(x_c \geq x_{sl} \rightarrow v_c \leq v_{sl}\big) \land \big(x_c \geq x_i - D \land x_c \leq x_i \rightarrow (x_{sl} \leq x_i \lor v_c \leq v_{sl})\big)\Big)$$

$$vsli \equiv (ctrl; dyn)^*$$

$$ctrl \equiv ctrl_{car} || ctrl_{ctr}$$

$$ctrl_{ctr} \equiv \text{if } (\neg Alert_\varepsilon) \text{ then } (x_{sl} := x_{sl};\ v_{sl} := v_{sl}) \cup \big(x_{sl} := *;\ v_{sl} := *; ?(v_{sl} \geq 0 \land Safe_{\underline{sl}})\big)$$
$$\text{else } x_{sl} := *;\ v_{sl} := *; ?(v_{sl} \geq v_{min} \land Safe_{\underline{sl}} \land Safe_{\overline{sl}}) \text{ fi;}$$

$$Alert_\varepsilon \equiv \boxed{x_i - D \leq x_c} + \left(\frac{v_c^2 - v_{min}^2}{2 \cdot b} + \left(\frac{A}{b} + 1\right) \cdot \left(\frac{A}{2} \cdot \varepsilon^2 + \varepsilon \cdot v_c\right)\right) \cdot \left(1 + \frac{v_i}{v_{min}}\right) \land \boxed{x_c \leq x_i}$$

$$Safe_{\overline{sl}} \equiv (v_i = 0 \land x_{sl} \leq x_i) \lor \left(v_i > 0 \land \boxed{x_{sl} \leq \frac{x_i \cdot v_{min} + x_c \cdot v_i}{v_i + v_{min}}}\right)$$

$$dyn \equiv (t := 0; x_c' = v_c, v_c' = a_c, x_i' = -v_i, t' = 1 \,\&\, v_c \geq v_{min} \land t \leq \varepsilon)$$

Initial Conditions → [Model] Requirements

Traffic Control: Incident Warning

To Prove:

$$c \to \Box\, sl \to [vsli]\Big(\big(x_c \geq x_{sl} \to v_c \leq v_{sl}\big)$$

$$\wedge \big(x_c \geq x_i - D \wedge x_c \leq x_i \to (x_{sl} \leq x_i \vee v_c \leq v_{sl})\big)\Big)$$

✔ Verified in KeYmaera

$$vsli \equiv (ctrl; dyn)^*$$

$$ctrl \equiv ctrl_{car} || ctrl_{ctr}$$

$$ctrl_{ctr} \equiv \text{if } (\neg Alert_\varepsilon) \text{ then } (x_{sl} := x_{sl};\ v_{sl} := v_{sl}) \cup (x_{sl} := *;\ v_{sl} := *; ?(v_{sl} \geq 0 \wedge Safe_{\underline{sl}}))$$

$$\text{else } x_{sl} := *;\ v_{sl} := *; ?(v_{sl} \geq v_{min} \wedge Safe_{\underline{sl}} \wedge Safe_{\overline{sl}}) \text{ fi};$$

$$Alert_\varepsilon \equiv \boxed{x_i - D \leq x_c} + \left(\frac{v_c^2 - v_{min}^2}{2 \cdot b} + \left(\frac{A}{b} + 1\right) \cdot \left(\frac{A}{2} \cdot \varepsilon^2 + \varepsilon \cdot v_c\right)\right) \cdot \left(1 + \frac{v_i}{v_{min}}\right) \wedge \boxed{x_c \leq x_i}$$

$$Safe_{\overline{sl}} \equiv (v_i = 0 \wedge x_{sl} \leq x_i) \vee \left(v_i > 0 \wedge \boxed{x_{sl} \leq \frac{x_i \cdot v_{min} + x_c \cdot v_i}{v_i + v_{min}}}\right)$$

$$dyn \equiv (t := 0; x_c' = v_c, v_c' = a_c, x_i' = -v_i, t' = 1 \,\&\, v_c \geq v_{min} \wedge t \leq \varepsilon)$$

Initial Conditions → [Model] Requirements

Design Implications (Traffic center)

$$\boxed{x_i} - x_c \geq \left(\frac{v_c^2 - v_{sl}^2}{2 \cdot b} + \left(\frac{A}{b} + 1 \right) \cdot \left(\frac{A}{2} \cdot \varepsilon^2 + \varepsilon \cdot v_c \right) \right) \cdot \left(1 + \boxed{\frac{v_i}{v_{min}}} \right)$$

Traffic center must be able to measure or estimate **incident parameters**

- Position and velocity of incident

Assume **reasonable car behavior**

- Car is not allowed to wait for incident
- Unreasonably small minimum velocity results in large warning area

Design Implications (Driver assistance)

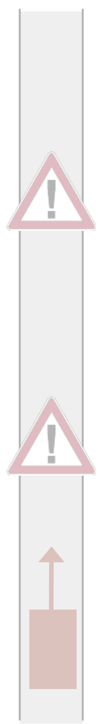
$$x_i - x_c \geq \left(\frac{v_c^2 - v_{sl}^2}{2 \cdot b} + \left(\frac{A}{b} + 1 \right) \cdot \left(\frac{A}{2} \cdot \varepsilon^2 + \varepsilon \cdot v_c \right) \right) \cdot \left(1 + \frac{v_i}{v_{min}} \right)$$

Fast-moving incidents **exceed local sensor range**

- 30m/s car and incident (e.g., wrong-way driver)
- 4m/s² accel., 9m/s² braking, 0.1s reaction
- **163m sensor range** for a complete stand still

Traffic Control: Incident Warning

Variable Speed Limit Control



1 vehicle
n traffic advice

Moving Incident Warning Control

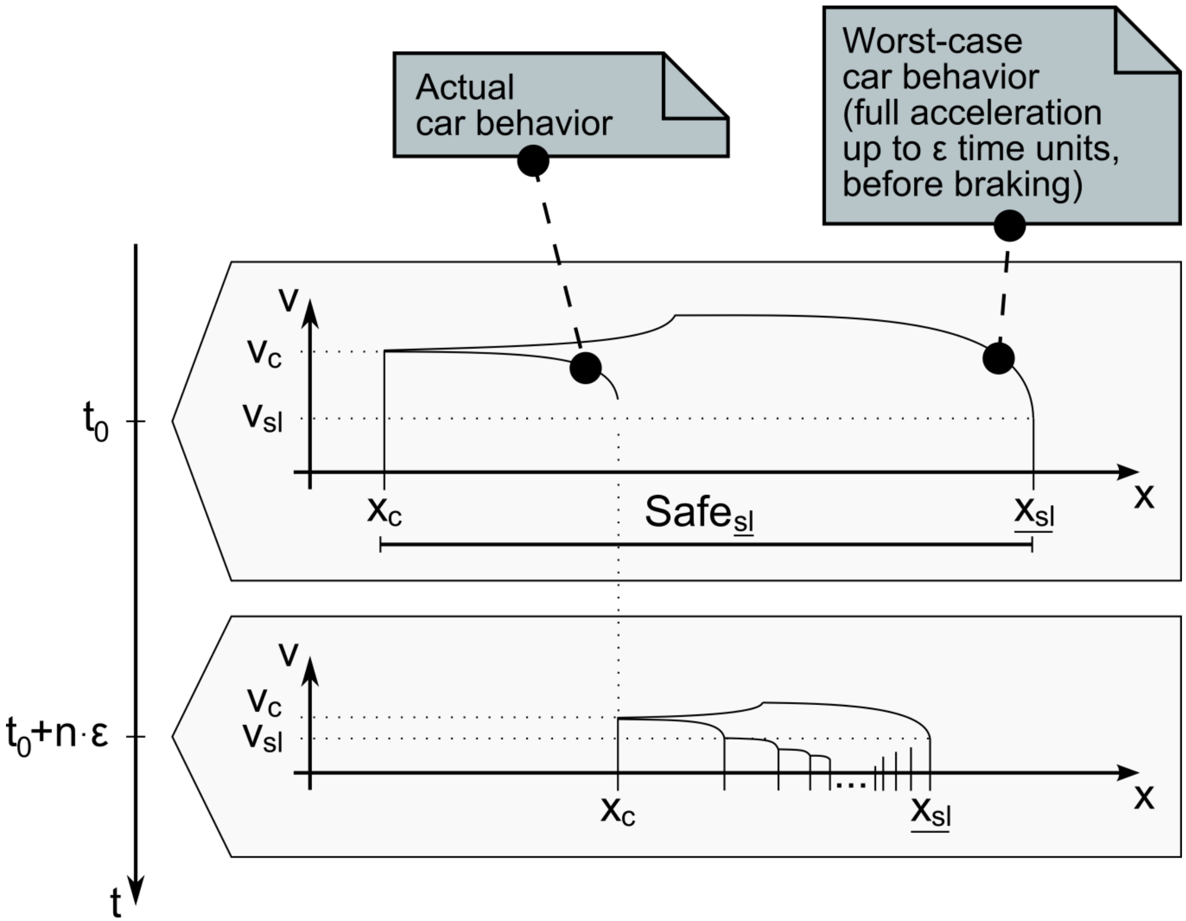
1 vehicle
1 incident
n traffic advice/warnings

Moving Incident Warning Control w/ Zeno Avoidance

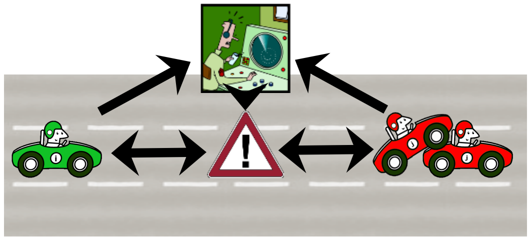
1 vehicles
1 incident
n traffic advice, 1 warning

Traffic Control: Incident Warning

Avoid Zeno-type effects when warning cars



Conclusions



Closed-loop traffic control: cope with limited local sensor coverage **globally** in traffic centers

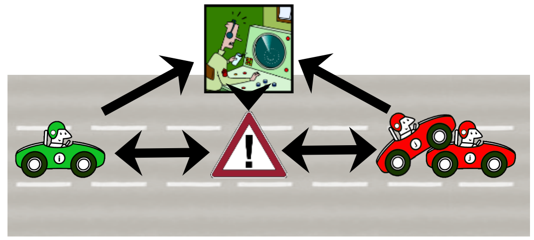
- **Incidents,** may move towards cars

Traffic control models are **formally verified**

Derive design decisions from verified models

- Image processing performance, camera resolution, etc.
- Local sensor range

Future Work



- Dedicated **up- and downlinks** for communication
- **Multiple control decisions** during one communication roundtrip
- **Advanced physical models** (curves, road conditions, etc.)
- **Collaborative, global control** actions in a fleet of cars (V2V communication)

Reference

For the full paper see:

Stefan Mitsch, Sarah M. Loos, and André Platzer. Towards Formal Verification of Freeway Traffic Control. In *International Conference on Cyber-Physical Systems, ICCPS, Beijing, China*, April 17-19. 2012.