Formalization and Improvements to the Responsibility-Sensitivity Safety Model for Self-Driving Cars

Megan Strauss

15-424 Logical Foundations of Cyber Physical Systems/Independent Study
The RSS Model
Introduction to RSS

- Protocol for self driving cars to follow to avoid collision
- Safe and scalable
- No car driving under this model would be the cause of an accident[1]
Coordinate System

- Lateral position - distance from center of lane
- Longitudinal position - distance travelled on the road
Safe Distance

- Two cars driving in the same longitudinal direction
  
  \[ d_{\text{min}, y} = \max \left( v_1 \rho + \frac{1}{2} a_{\text{maxAccel}}^\text{long} \rho^2 + \frac{(v_1 + \rho a_{\text{maxAccel}}^\text{long})^2}{2a_{\text{minBrake}}^\text{long}} - \frac{v_2^2}{2a_{\text{maxBrake}}^\text{long}}, 0 \right) \]

- Two cars driving in opposite longitudinal directions
  
  \[ d_{\text{min}, y} = \frac{v_1 + v_1 \rho}{2} \rho + \frac{(v_1 \rho)^2}{2a_{\text{minBrakeCorrect}}^\text{long}} + \frac{|v_2| + v_2 \rho}{2} \rho + \frac{(v_2 \rho)^2}{2a_{\text{minBrake}}^\text{long}} \]

- The lateral safe distance
  
  \[ d_{\text{min}, x} = \mu + \min \left( \frac{v_1 + v_1 \rho}{2} \rho + \frac{(v_1 \rho)^2}{2a_{\text{minBrake}}^\text{lat}} - \left( \frac{v_2 + v_2 \rho}{2} \rho + \frac{(v_2 \rho)^2}{2a_{\text{minBrake}}^\text{lat}} \right) \right) \]
Proper Response

1. For $\rho$ time continue accelerating at any rate
2. After $\rho$ time in an unsafe, perform proper response until distance is safe again
Example: Proper Response for Opposite Longitudinal Direction
Formalizing the Model
3 Models

- Two cars driving in the same longitudinal direction
- Two cars driving in opposite longitudinal direction
- Two cars driving in same or opposite lateral directions
Controller/Continuous Dynamics

- **Idea**
  - While distance is safe, accelerate at any rate
  - If distance becomes unsafe, perform proper response
- **In KeymaeraX**

```plaintext
{{
  /*Choose which controller to use based on distance*/
  ??safeDist(v1, v2)<=x2-x1; Control;
  ++ ??safeDist(v1, v2)>=x2-x1; ProperResponse;}
}}
```
- Assumes cars follow basic kinematics

\[
x_1' = v_1, \quad x_2' = v_2, \quad v_1' = a_1, \quad v_2' = a_2
\]
Time-Triggered Model
Controller

- Idea
  - Check that distance is safe for all times in between current time and next time that distance is computed (different for each case)
  - If distance is unsafe at any point, start proper response
    - Proper response behavior can always be done
Time-Triggered Case for Cars Driving in Opposite Directions

- Check that current distance is safe
- Check that if cars drive for maximum amount of time, distance will be safe
- In KeymaeraX

/*If current position or position in T time points is unsafe, run proper response, else run control*/

{?safeDist(v1, v2)<=x2-x1
 & safeDist(v1 + T*aMaxAccel , v2 - T*aMaxAccel)<=
 (x2 + v2*T - aMaxAccel*T/2) - (x1 + v1*T + aMaxAccel*T/2);
  control;}

++

{?safeDist(v1, v2)>=x2-x1
 | safeDist(v1 + T*aMaxAccel , v2 - T*aMaxAccel)
 >= (x2 + v2*T - aMaxAccel*T/2) - (x1 + v1*T + aMaxAccel*T/2);
  longProperResponseOpposite; }*
Results
Proven Models

- Original (event-triggered) model for opposite longitudinal directions
- Time-triggered model for opposite longitudinal directions
- Original (event-triggered) model for lateral movement
- Time-triggered model for lateral movement
Unproven model

- Unproven model is the case with two cars travelling in the same direction.
- Current safe distance metric for this case is derived from kinematics based on positions that both cars would stop, which does not imply that the cars will not collide before stopping.
Future work/applications

- Find a new lower bound for the case of cars driving the same direction
- Beyond this
  - Self driving cars make the world more convenient and safer
  - This model pushes towards safe and scalable self driving cars.
Sources
