MODELING AND FORMAL VERIFICATION OF VEHICLE PLATOONING SYSTEM

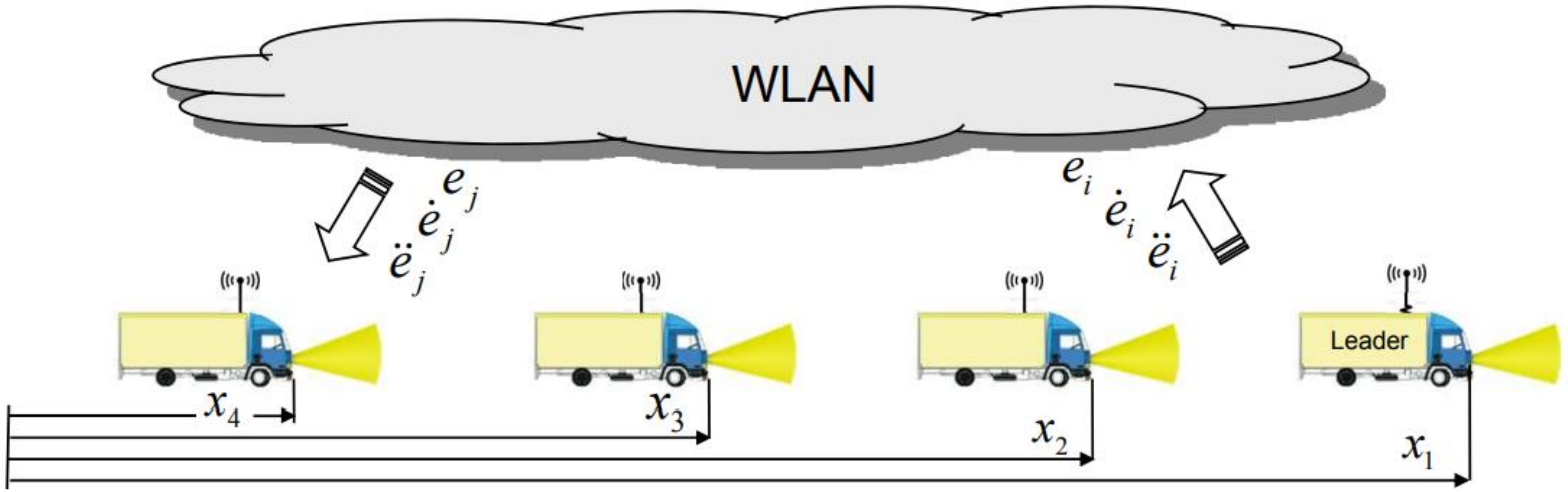
PRESENTED BY: PROMIT PANJA

Outline

- Introduction
- Background
- System Model
- Verification
- Conclusion

Introduction

- The operation of group of vehicles at small inter-vehicular distances is known as **vehicle platooning.**



Introduction

- Need for platooning?

Some studies show driving heavy-vehicles in a platoon **reduces** aerodynamic drag and **reduces** fuel consumption by up to **10%**.

At a high level

- We take a ***cyber-physical*** systems approach to model and verify such a system.
- Building mathematical models of dynamical systems characterized by multiple facets like **discrete**, **continuous**, **adversarial**, **non-determinism**, and **stochastic**.
- Formally verify these models using **mathematical proof theory** and **axiomatization**.

Background

- Differential Dynamic Logic (dL)

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

$$\phi ::= \theta_1 \sim \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x \phi \mid \exists x \phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi$$

Background

- Hybrid Program (HP)

$$\alpha, \beta \ ::= x \coloneqq e \mid ?\,Q \mid x' = f(x)\&Q \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^*$$

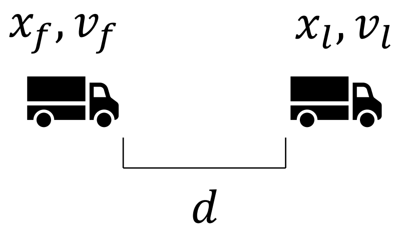
$$dL \ ::= \underbrace{\color{red}{Initial\ Conditions}}_{\text{Logic Formula}} \ \rightarrow [\underbrace{Model}_{\substack{\text{Hybrid Program} \\ \textit{(ctrl;dyn)*}}}]\ \underbrace{\color{red}{Post\ Condition}}_{\text{Logic Formula}}$$

Background

Statement	Effect
$\alpha;\ \beta$	sequential composition, first performs α and then β afterwards
$\alpha\ \cup\ \beta$	nondeterministic choice, following either α or β
α^*	nondeterministic repetition, repeating α $n \geq 0$ times
$x := \theta$	discrete assignment of the value of term θ to variable x (jump)
$x := *$	nondeterministic assignment of an arbitrary real number to x
$(x_1' = \theta_1, \ldots,$ $x_n' = \theta_n\ \&\ F)$	continuous evolution of x_i along differential equation system $x_i' = \theta_i$, restricted to maximum domain or invariant region F
$?F$	check if formula F holds at current state, abort otherwise
if(F) then α else β	perform α if F holds, perform β otherwise

System Model

- Two Vehicle Highway Platoon



Lead Vehicle: l, Follower Vehicle: f

$$x_l - x_f \geq d$$

$$x' = v, v' = a, t' = 1$$

$$A \geq 0$$

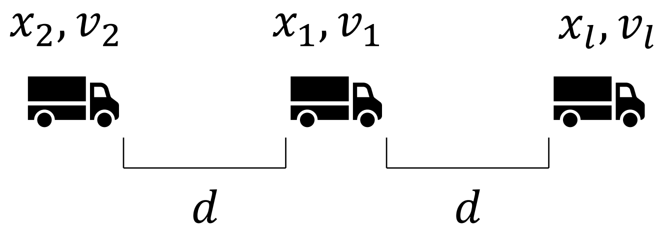
$$B \geq b > 0$$

System Model

$$
\begin{aligned}
&hp \equiv (ctrl; dyn)^* \\
&ctrl \equiv l_{ctrl} || f_{ctrl}; \\
&l_{ctrl} \equiv (a_l := *; ?(-B \leq a_l \leq A)) \\
&f_{ctrl} \equiv (a_f := *; ?(-B \leq a_l \leq A)) \\
&\cup (?\mathbf{Safe}_\delta; a_f := *; ?(-B \leq a_l \leq A)) \\
&\cup (?(v_f = 0); a_f := 0) \\
&\mathbf{Safe}_\delta \equiv x_f + \frac{v_f^2}{2b} + (\frac{A}{b} + 1)(\frac{A}{2}\delta^2 + \delta v_f) < x_l + \frac{v_l^2}{2B} \\
&dyn \equiv (t := 0; x_f' = v_f, v_f' = a_f, x_l' = v_l, v_l' = a_l, \\
&v_f \geq 0 \wedge v_l \geq 0 \wedge t \leq \delta)
\end{aligned}
$$

System Model

- Three Vehicle Highway Platoon



Lead Vehicle: l, Follower Vehicle 1: f_1, Follower Vehicle 2: f_2

$$x_l - x_1 \geq d, x_1 - x_2 \geq d$$

$$x' = v, v' = a, t' = 1$$

$$A \geq 0$$

$$B \geq b > 0$$

System Model

$$hp \equiv (ctrl; dyn)^*$$
$$ctrl \equiv l_{ctrl} || f_{ctrl1} || f_{ctrl2};$$
$$l_{ctrl} \equiv (a_l := *; ?(-B \leq a_l \leq A))$$
$$f_{ctrl1} \equiv (a_1 := *; ?(-B \leq a_l \leq A))$$
$$\cup (?\mathbf{Safe}_\delta; a_1 := *; ?(-B \leq a_l \leq A))$$
$$\cup (?(v_1 = 0); a_1 := 0)$$
$$f_{ctrl2} \equiv (a_2 := *; ?(-B \leq a_1 \leq A))$$
$$\cup (?\mathbf{Safe}_\delta; a_2 := *; ?(-B \leq a_1 \leq A))$$
$$\cup (?(v_2 = 0); a_2 := 0)$$
$$\mathbf{Safe}_\delta \equiv x_1 + \frac{v_1^2}{2b} + (\frac{A}{b} + 1)(\frac{A}{2}\delta^2 + \delta v_1) < x_l + \frac{v_l^2}{2B}$$
$$\mathbf{Safe}_\delta \equiv x_2 + \frac{v_2^2}{2b} + (\frac{A}{b} + 1)(\frac{A}{2}\delta^2 + \delta v_2) < x_1 + \frac{v_1^2}{2B}$$
$$dyn \equiv (t := 0; x_2' = v_2, v_2' = a_2, x_1' = v_1, v_1' = a_1,$$
$$x_l' = v_l, v_l' = a_l v_1 \geq 0 \wedge v_2 \geq 0 \wedge v_l \geq 0 \wedge t \leq \delta)$$

Verification

To formally verify we use **axioms**, **proof rules**, and **theorems**.

eg. Godel’s Generalization Rule, Tarski’s Quantifier Elimination Rule, Sequent Calculi, etc.

Can be proved using software tools like **KeYmaera X**, **Hal**, etc.

Verification

TwoVehiclesLinear

New proof Edit

```
Theorem "TwoVehiclesLinear"

Definitions
    Real A;
    Real B;
    Real b;
    Real td;
    Real d;
End.

ProgramVariables
    Real xl;
    Real vl;
    Real al;

    Real xf;
    Real vf;
    Real af;

    Real t;
End.


Problem
  /* INITIAL CONDITIONS */
  (xf < xl & xl - xf >= d & xl > xf + (vf^2)/(2*b) + (A/b + 1)*((A/2)*(td^2) + td*vf) - (vl^2)/(2*b) & B >= b & b > 0 & vf >= 0 & vl >= 0 & A >= 0 & td >= 0)
  ->
  [
    {
        /*CONTROL*/
        {
            {al := *; ?(-B <= al & al <= A);}                /*LEAD VEHICLE*/
            {af := *; ?(-B <= af & af <= A); ++ ?(xl > xf + (vf^2)/(2*b) + (A/b + 1)*((A/2)*(td^2) + td*vf) - (vl^2)/(2*b)); af := *; ?(-B <= af & af <= A); ++ ?vf = 0; af := 0;} /*FOLLOWER
        }
        t := 0;
        /*CONTINUOUS DYNAMICS*/
        {
            {xl' = vl, vl' = al, xf' = vf, vf' = af, t' = 1 & vl >= 0 & vf >= 0 & t <= td }
        }
    }*@invariant(xf < xl & xl - xf >= d & xf + (vf^2)/(2*b) + (A/b + 1)*((A/2)*(td^2) + td*vf) < xl + (vl^2)/(2*B) & vf >= 0 & vl >= 0)

    ](xf < xl & xl - xf >= d & xf + (vf^2)/(2*b) + (A/b + 1)*((A/2)*(td^2) + td*vf) < xl + (vl^2)/(2*B) & vf >= 0 & vl >= 0)
```

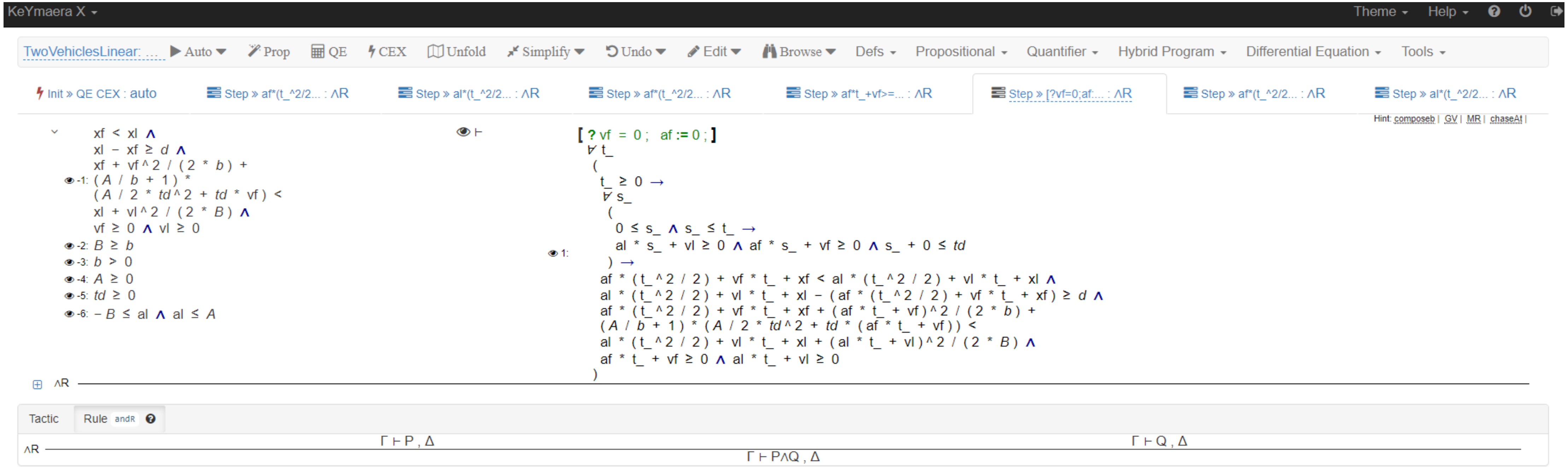
Verification

ThreeVehiclesLinear

New proof | Edit

```
Theorem "ThreeVehiclesLinear"

Definitions
    Real A;
    Real B;
    Real b;
    Real td;
    Real d;
End.

ProgramVariables
    Real xl;
    Real vl;
    Real al;

    Real x1;
    Real v1;
    Real a1;

    Real x2;
    Real v2;
    Real a2;

    Real t;
End.


Problem
  /* INITIAL CONDITIONS */
  (x2 < x1 & x1 - x2 >= d & x1 < xl & xl - x1 >= d & x1 > x2 + (v2^2)/(2*b) + (A/b + 1)*((A/2)*(td^2) + td*v2) - (v1^2)/(2*b) & xl > x1 + (v1^2)/(2*b) + (A/b + 1)*((A/2)*(td^2) + td*v1) - (
  ->
  [
    {
      /*CONTROL*/
      {
        {al := *; ?(-B <= al & al <= A);}                /*LEAD VEHICLE*/
        {a1 := *; ?(-B <= a1 & a1 <= A); ++ ?(xl > x1 + (v1^2)/(2*b) + (A/b + 1)*((A/2)*(td^2) + td*v1) - (vl^2)/(2*b)); a1 := *; ?(-B <= a1 & a1 <= A); ++ ?v1 = 0; a1 := 0;} /*FOLLOWER
        {a2 := *; ?(-B <= a2 & a2 <= A); ++ ?(x1 > x2 + (v2^2)/(2*b) + (A/b + 1)*((A/2)*(td^2) + td*v2) - (v1^2)/(2*b)); a2 := *; ?(-B <= a2 & a2 <= A); ++ ?v2 = 0; a2 := 0;} /*FOLLOWER
      }
      t := 0;
      /*CONTINUOUS DYNAMICS*/
      {
```

Verification



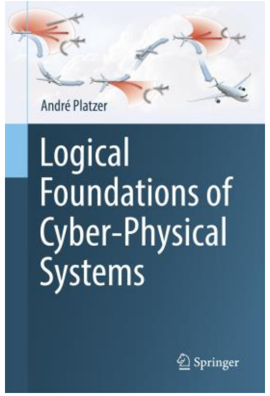
Conclusion & Future Work

- Formally proven the **linear** platoon models.
- Vehicle dynamics such as **non-linear path**, **computation latency**, **drag**, etc. Need to be incorporated.
- Can also be modeled using **state-space analysis (automata theory)** using softwares like LabView, Simulink, Hsolver, etc.
- Control optimizations like **Model Predictive Control (MPC)** which work well with machine perception.

Annexure

- Logical Foundations of Cyber-Physical Systems by A. Platzer

  https://lfcps.org/lfcps/



- KeYmaera X: An aXiomatic Tactical Theorem Prover for Hybrid Systems

  https://keymaerax.org/

Questions?

Thank You!